

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-063147

(43)Date of publication of application : 28.02.2002

(51)Int.Cl.

G06F 15/177

H04L 9/10

(21)Application number : 2000-247230

(71)Applicant : SONY CORP

(22)Date of filing : 17.08.2000

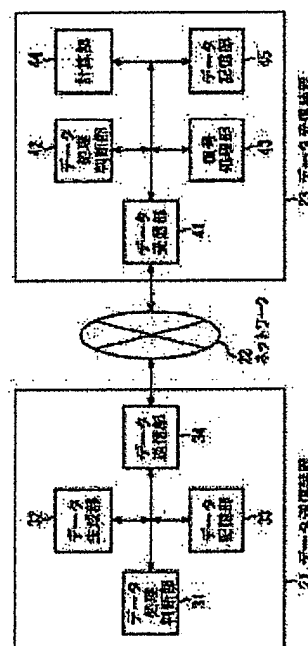
(72)Inventor : MUTO AKIHIRO

(54) DEVICE FOR PROCESSING INFORMATION, METHOD FOR THE SAME AND RECORDING MEDIUM

(57)Abstract:

**PROBLEM TO BE SOLVED:** To ensure processing performance for decoding enciphered contents data.

**SOLUTION:** A data receiver 23 for receiving and decoding contents data transmitted from a data transmitter 21 confirms the contents of meta data, in which information related with the encipherment of the contents data is described, before processing the contents data. A decoding processing part 43 compares the processing contents requested by the meta data with own processing performance, and when the requested processing cannot be achieved is decided when the decoding is performed by the decoding processing part 43 alone, the decoding processing part 43 requests a calculating part 44 to conduct dispersion processing of the contents data. The decoding processing part 43 receives and conducts the dispersion and decoding of the contents data, when the authentication of the dispersion processing is established with the calculating part 44, which is requested to conduct the dispersion processing.



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号  
特開2002-63147  
(P2002-63147A)

(43) 公開日 平成14年2月28日 (2002.2.28)

(51) Int.Cl. <sup>7</sup>	識別記号	F I	テームコード* (参考)
G 0 6 F 15/177	6 7 4	G 0 6 F 15/177	6 7 4 A 5 B 0 4 5
H 0 4 L 9/10		H 0 4 L 9/00	6 2 1 Z 5 J 1 0 4

審査請求 未請求 請求項の数 4 O L (全 27 頁)

(21) 出願番号 特願2000-247230 (P2000-247230)

(22) 出願日 平成12年8月17日 (2000.8.17)

(71) 出願人 000002185

ソニー株式会社

東京都品川区北品川6丁目7番35号

(72) 発明者 武藤 明宏

東京都品川区北品川6丁目7番35号 ソニー株式会社内

(74) 代理人 100082131

弁理士 稲本 義雄

Fターム(参考) 5B045 GG01

5J104 AA09 AA32 LA01 LA05 LA06

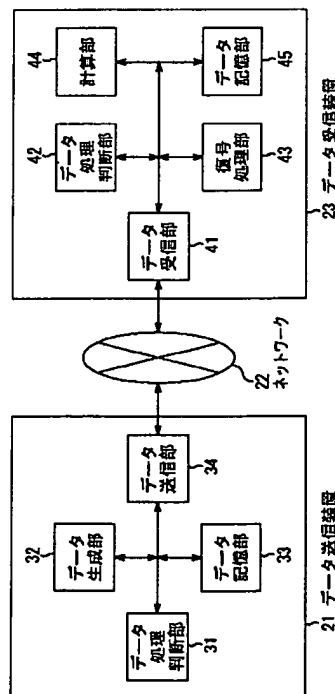
PA07 PA11 PA14

(54) 【発明の名称】 情報処理装置、情報処理方法、並びに記録媒体

(57) 【要約】

【課題】 暗号化されたコンテンツデータを復号する処理能力を確保する。

【解決手段】 データ送信装置21から送信されるコンテンツデータを受信して復号処理するデータ受信装置23は、コンテンツデータを受信する前に、コンテンツデータの暗号化に関する情報が記述されているメタデータの内容を確認する。復号処理部43は、メタデータにより要求される処理内容と、自分自身の処理能力を比較し、復号処理部43が単独で復号処理を行ったのでは、要求される処理を行うことができないと判定した場合、計算部44に対して、コンテンツデータを分散して処理することを要求する。復号処理部43は、分散処理を要求した計算部44との間で分散処理の認証が成立した場合、コンテンツデータを受信し、分散して復号処理する。



## 【特許請求の範囲】

【請求項1】 コンテンツデータと、その特徴に関する情報が記述されている特徴情報を受信する受信手段と、前記受信手段により受信された前記特徴情報から、前記コンテンツデータのデータ処理に要求される処理能力を認識する認識手段と、

前記認識手段により認識された前記データ処理に要求される処理能力と、自分自身の処理能力を比較する比較手段と、

前記比較手段により比較された自分自身の処理能力が、前記データ処理に要求される処理能力を充足していないと判断された場合、所定のデータ処理部だけでなく、他のデータ処理部に前記データ処理を委託し、前記コンテンツデータを分散処理する分散処理手段とを含むことを特徴とする情報処理装置。

【請求項2】 前記他のデータ処理部の前記データ処理が、前記所定のデータ処理部が分散処理を委託する処理要求に基づいて実行されているか否かを判断する判断手段をさらに含むことを特徴とする請求項1に記載の情報処理装置。

【請求項3】 コンテンツデータと、その特徴に関する情報が記述されている特徴情報を受信する受信ステップと、

前記受信ステップの処理により受信された前記特徴情報から、前記コンテンツデータのデータ処理に要求される処理能力を認識する認識ステップと、

前記認識ステップの処理により認識された前記データ処理に要求される処理能力と、自分自身の処理能力を比較する比較ステップと、

前記比較ステップの処理により比較された自分自身の処理能力が、前記データ処理に要求される処理能力を充足していないと判断された場合、所定のデータ処理部だけでなく、他のデータ処理部に前記データ処理を委託し、前記コンテンツデータを分散処理する分散処理ステップとを含むことを特徴とする情報処理方法。

【請求項4】 コンテンツデータと、その特徴に関する情報が記述されている特徴情報を受信する受信ステップと、

前記受信ステップの処理により受信された前記特徴情報から、前記コンテンツデータのデータ処理に要求される処理能力を認識する認識ステップと、

前記認識ステップの処理により認識された前記データ処理に要求される処理能力と、自分自身の処理能力を比較する比較ステップと、

前記比較ステップの処理により比較された自分自身の処理能力が、前記データ処理に要求される処理能力を充足していないと判断された場合、所定のデータ処理部だけでなく、他のデータ処理部に前記データ処理を委託し、前記コンテンツデータを分散処理する分散処理ステップとを含むことを特徴とするコンピュータが読みとり可能

なプログラムが記録されている記録媒体。

## 【発明の詳細な説明】

## 【0001】

【発明の属する技術分野】本発明は、情報処理装置、情報処理方法、並びに記録媒体に関し、特に、暗号化されたコンテンツデータのデータ処理を、他のデータ処理部と分散して処理することにより、システム毎に設計したハードウェアを用いることなく、迅速にデータを処理することを可能にした情報処理装置、情報処理方法、並びに記録媒体に関する。

## 【0002】

【従来の技術】近年、コンテンツデータをネットワークを介して配信する配信システムが構築されている。配信されるコンテンツデータは、データの改竄を防ぐため、暗号化や、デジタル署名を付加するなどの処理が施されている。暗号化されたコンテンツデータは、利用者の端末により復号処理され、利用者はそれを利用することができる。

【0003】暗号化技術の安全性は、復号する際の処理の難しさに依存しているため、暗号化技術の高度化にともなって、コンテンツデータを利用する利用者の端末には、より処理能力の高い端末が要求されるようになっていく。

【0004】そこで、処理能力を確保するために、利用者端末に復号処理専用のLSI (Large Scale Integration) を配置することが考えられる。図1は、復号処理専用のLSI (以下、復号LSIと称する)の構成例を示している。

【0005】復号LSI 1は、復号LSI 1の外部に配置されるコントロールマイクロコンピュータ (以下、コントロールマイコンと略称する) 2から転送される指令により復号処理を行う。復号処理には、暗号化されたコンテンツデータを復号する処理の他に、コンテンツデータに付加されているデジタル署名を検証する処理が含まれる。復号LSI 1が処理した結果は、復号LSI 1の外部に配置される外部メモリ 3に記憶される。

【0006】復号LSI 1は、通信インタフェース 11、コントロールユニット 12、RAM (Random Access Memory) 13、メモリコントローラ 14、フラッシュメモリ 15、べき乗演算器 16、ハッシュ値演算器 17から構成される。

【0007】コントロールマイコン 2から転送される指令は、通信インタフェース 11を介してコントロールユニット 12に伝えられる。コントロールユニット 12は、べき乗演算器 16およびハッシュ値演算器 17などを補助的に用いつつ、復号LSI 1の全体の動作を制御し、暗号化されているデータの復号処理、およびデジタル署名の検証処理などを行う。

【0008】RAM 13には、コントロールユニット 12が利用するプログラムが記憶されている。

10

20

30

40

50

【0009】メモリコントローラ14は、外部メモリ3に対するデータの読み書きを制御する。

【0010】フラッシュメモリ15には、コントロールユニット12の指令によりべき乗演算器16、およびハッシュ値演算器17が演算した結果や、処理に必要なデータが、適宜、記憶される。

【0011】利用者が使用する端末に、上述したような復号LSI1を配置することにより、コンテンツデータの復号処理能力を確保することが可能となる。

【0012】

【発明が解決しようとする課題】しかしながら、利用者端末に復号LSI1（ハードウェア）を設置する場合、暗号化されたコンテンツデータの復号処理能力は、暗号化のセキュリティレベルに応じて計算量が異なるため、最大の負荷を処理することができるように復号LSI1を構成する必要がある。その結果、コスト高となる課題があった。また、処理能力を変更する必要がある場合、LSIを設計し直す必要があるため、バージョンアップ等の変更が実質的に困難になる課題があった。

【0013】本発明はこのような状況に鑑みてなされたものであり、暗号化されたコンテンツデータを利用者端末において復号する場合に、システム毎に設計したハードウェアを利用することなく、低コストで、かつ、比較的容易に機能を変更できるシステムを実現できるようにするものである。

【0014】

【課題を解決するための手段】本発明の情報処理装置は、コンテンツデータと、その特徴に関する情報が記述されている特徴情報を受信する受信手段と、受信手段により受信された特徴情報から、コンテンツデータのデータ処理に要求される処理能力を認識する認識手段と、認識手段により認識されたデータ処理に要求される処理能力と、自分自身の処理能力を比較する比較手段と、比較手段により比較された自分自身の処理能力が、データ処理に要求される処理能力を充足していないと判断された場合、所定のデータ処理部だけでなく、他のデータ処理部にデータ処理を委託し、コンテンツデータを分散処理する分散処理手段とを含むことを特徴とする。

【0015】本発明の情報処理装置は、前記他のデータ処理部のデータ処理が、所定のデータ処理部が分散処理を委託する処理要求に基づいて実行されているか否かを判断する判断手段をさらに含むようにすることができる。

【0016】本発明の情報処理方法は、コンテンツデータと、その特徴に関する情報が記述されている特徴情報を受信する受信ステップと、受信ステップの処理により受信された特徴情報から、コンテンツデータのデータ処理に要求される処理能力を認識する認識ステップと、認識ステップの処理により認識されたデータ処理に要求される処理能力と、自分自身の処理能力を比較する比較ス

テップと、比較ステップの処理により比較された自分自身の処理能力が、データ処理に要求される処理能力を充足していないと判断された場合、所定のデータ処理部だけでなく、他のデータ処理部にデータ処理を委託し、コンテンツデータを分散処理する分散処理ステップとを含むことを特徴とする。

【0017】本発明の記録媒体のプログラムは、コンテンツデータと、その特徴に関する情報が記述されている特徴情報を受信する受信ステップと、受信ステップの処理により受信された特徴情報から、コンテンツデータのデータ処理に要求される処理能力を認識する認識ステップと、認識ステップの処理により認識されたデータ処理に要求される処理能力と、自分自身の処理能力を比較する比較ステップと、比較ステップの処理により比較された自分自身の処理能力が、データ処理に要求される処理能力を充足していないと判断された場合、所定のデータ処理部だけでなく、他のデータ処理部にデータ処理を委託し、コンテンツデータを分散処理する分散処理ステップとを含むことを特徴とする。

【0018】本発明の情報処理装置、情報処理方法、および記録媒体のプログラムにおいては、コンテンツデータと、その特徴に関する情報が記述されている特徴情報が受信され、受信された特徴情報から、コンテンツデータのデータ処理に要求される処理能力が認識される。また、認識されたデータ処理に要求される処理能力と、自分自身の処理能力が比較され、自分自身の処理能力が、データ処理に要求される処理能力を充足していないと判断された場合、所定のデータ処理部だけでなく、他のデータ処理部にデータ処理が委託され、コンテンツデータが分散処理される。

【0019】

【発明の実施の形態】図2は、本発明を適用したデータ処理システムの構成例を示すブロック図である。データ送信装置21により生成され、暗号化されたコンテンツデータは、ネットワーク22を介してデータ受信装置23に送信される。

【0020】データ送信装置21は、データ処理判断部31、データ生成部32、データ記憶部33、およびデータ送信部34から構成される。

【0021】データ処理判断部31は、データ送信装置21の全体の動作を制御する。データ生成部32は、所定の方法により提供されたコンテンツデータを暗号化したり、デジタル署名を生成する（以下、コンテンツデータの暗号化処理、およびデジタル署名の生成処理をまとめて暗号関連処理と称する）。また、データ生成部32は、コンテンツデータの暗号化に関するデータなどが記述されているメタデータを生成する。データ記憶部33は、データ生成部32により生成されたコンテンツデータおよびメタデータを記憶する。データ送信部34は、データ受信装置23からの要求に応じて、データ記

憶部33に記憶されているメタデータおよびコンテンツデータを送信する。

【0022】ネットワーク22は、データ送信装置21およびデータ受信装置23の間で送受信されるデータの伝送路であり、例えば、インターネット、電話回線網、ケーブルテレビジョン放送網、衛星を介したデジタルテレビジョン放送網等により構成される。

【0023】データ受信装置23は、データ受信部41、データ処理判断部42、復号処理部43、計算部44、およびデータ記憶部45より構成される。

【0024】データ受信部41は、データ送信装置21から送信されたメタデータおよびコンテンツデータを受信する。データ処理判断部42は、データ受信装置23の全体の動作を制御する。復号処理部43は、データ受信部41により受信されたコンテンツデータが暗号化されている場合にはコンテンツデータを復号し、デジタル署名が付加されている場合には、デジタル署名の検証などの処理を行う（以下、コンテンツデータの復号処理、およびデジタル署名の検証処理をまとめて復号関連処理と称する）。計算部44は、データ処理判断部42の指令を受けて、演算処理機能を提供する。データ記憶部45は、データ受信部41により受信されたコンテンツデータ、および復号処理部43により復号され、かつデジタル署名が検証されたコンテンツデータを記憶する。

【0025】次に、データ送信装置21が送信するメタデータおよびコンテンツデータを、データ受信装置23が受信し、処理する一連の処理について、図3乃至図5のフローチャートを参照して説明する。

【0026】図3は、データ送信装置21の処理を説明するフローチャートである。ステップS1において、データ生成部32は、外部から所定の方法により提供されるアナログデータまたはデジタルデータを取得し、コンテンツデータを作成する。データ生成部32は、ネットワーク22を介してデータ受信装置23に対して送信することが可能な形式に圧縮し、暗号関連処理を施して、コンテンツデータを作成する。

【0027】また、データ生成部32は、メタデータを生成する。メタデータには、送信されるコンテンツデータの特徴、コンテンツデータの暗号関連処理に関する情報である暗号関連情報が記述される。コンテンツデータの特徴には、例えば、コンテンツデータの制作者、制作時期、制作者を識別する制作者ID、コンテンツデータの利用形態、コンテンツデータ利用形態毎の料金、コンテンツデータの再生時間、コンテンツデータの圧縮方法、総データ量、データの転送速度などが含まれる。また、コンテンツデータの暗号関連情報には、例えば、暗号化アルゴリズム、デジタル署名の生成アルゴリズム、データ単位が含まれる。これらの具体例については後述する。

【0028】ステップS2において、データ記憶部33は、ステップS1の処理でデータ生成部32により作成されたコンテンツデータおよびメタデータを記憶する。

【0029】ステップS3において、データ処理判断部31は、データ受信装置23からメタデータの送信が要求されたか否かを判定し、メタデータの送信が要求されたと判定するまで待機する。データ処理判断部31によりメタデータの送信が要求されたと判定された場合、処理はステップS4に進む。

10 【0030】ステップS4において、データ送信部34は、データ記憶部33に記憶されているメタデータを、ネットワーク22を介してデータ受信装置23に送信する。後述するように、メタデータを受信したデータ受信装置23は、メタデータに記述されている情報を分析し、コンテンツデータの処理を準備する。メタデータに記述されているコンテンツデータの情報に応じて、コンテンツデータを処理する準備が完了した場合、データ受信装置23は、コンテンツデータの送信をデータ送信装置21に要求する。

20 【0031】そこで、ステップS5において、データ処理判断部31は、データ受信装置23からコンテンツデータの送信が要求されたか否かを判定する。

【0032】ステップS5において、データ処理判断部31によりデータ受信装置23からコンテンツデータの送信が要求されていないと判定された場合、データ処理判断部31は、データ受信装置23が、コンテンツデータの処理の準備が完了していないと認識し、コンテンツデータの送信が要求されるまで待機する。

30 【0033】ステップS5において、データ処理判断部31が、データ受信装置23からコンテンツデータの送信が要求されたと判定した場合、処理はステップS6に進み、データ送信部34は、データ記憶部33に記憶されているコンテンツデータを、ネットワーク22を介してデータ受信装置23に対して送信する。

【0034】図4および図5は、データ受信装置23の処理を説明するフローチャートである。ステップS11において、データ処理判断部42は、データ受信装置23を管理する利用者からコンテンツデータの受信の指令が入力された場合、データ送信装置21に対して、そのコンテンツデータに対応するメタデータの送信を要求する。

40 【0035】ステップS12において、データ受信部41は、データ送信装置21から送信されてきたメタデータを、ネットワーク22を介して受信する。データ受信部41が受信したメタデータは、データ処理判断部42に転送され、データ処理判断部42により記述されている内容が分析される。

50 【0036】ステップS13において、データ処理判断部42は、メタデータに記述されているコンテンツデータの情報から、送信されてくるコンテンツデータは、暗

号関連処理が施されているか否かを判定する。

【0037】ステップS13において、データ処理判断部42は、送信されてくるコンテンツデータには、暗号関連処理が施されていないと判定した場合、処理はステップS14に進み、データ処理判断部42は、データ送信装置21に対して、コンテンツデータの送信を要求する。

【0038】ステップS15において、データ受信部41は、データ送信装置21から、ネットワーク22を介して送信されたコンテンツデータを受信する。データ受信装置23を管理する利用者がデータ受信部41により受信されたコンテンツデータを利用する場合、コンテンツデータは復号関連処理を行う必要がないため、データ記憶部45は、コンテンツデータを記憶し、データ受信装置23を管理する利用者から要求があるまで保持する。

【0039】一方、ステップS13において、データ処理判断部42は、メタデータに記述されている内容から、送信されてくるコンテンツデータは暗号関連処理が施されているデータであると判定した場合、処理はステップS16に進む。

【0040】ステップS16において、データ処理判断部42は、コンテンツデータの暗号関連処理に関する情報である暗号関連情報を含むメタデータを復号処理部43に通知する。暗号関連情報には、コンテンツデータの暗号化アルゴリズム、デジタル署名のアルゴリズムおよびデータ単位が記述されている。復号処理部43は、コンテンツデータの暗号関連情報に基づいて、データ受信部41がコンテンツデータを受信した場合のコンテンツデータの復号関連処理を準備する。なお、データ処理判断部42により転送される暗号関連情報は、処理内容の漏洩、処理内容の改竄を防ぐために、さらに暗号関連処理が施されている場合があるが、ここでは、暗号関連情報には暗号関連処理が施されていないものとして説明する。

【0041】ステップS17において、復号処理部43は、データ受信部41により受信されたコンテンツデータの復号関連処理のうちの少なくとも一部を、他の処理部に委託する（分散処理する）必要があるか否かを判定する。この判定は、復号処理部43が、コンテンツデータの暗号化アルゴリズムに対応しているか否か、または、復号処理部43の暗号処理能力により、要求される時間内に復号関連処理を完了することが可能であるか否かなどを基準として行われる。

【0042】ステップS17において、復号処理部43が、コンテンツデータの分散処理は必要でないと判定した場合、すなわち、コンテンツデータの復号関連処理は復号処理部43が単独で行うことが可能であると判定した場合、処理はステップS18に進む。

【0043】ステップS18において、復号処理部43

から、コンテンツデータの復号関連処理の準備が完了した旨の通知を受けたデータ処理判断部42は、データ送信装置21に対して、コンテンツデータの送信を要求する。

【0044】ステップS19において、データ受信部41はコンテンツデータを受信する。受信されたコンテンツデータは、復号処理部43に転送され、復号処理部43は、単独で、コンテンツデータの復号関連処理を行う。復号関連処理が行われ、利用することが可能となったデータは、データ記憶部45に記憶される。

【0045】一方、ステップS17において、復号処理部43は、コンテンツデータを単独で復号関連処理を行うことができず、分散処理が必要であると判定した場合、処理はステップS20に進み、復号処理部43は分散処理の委託形式を決定し、決定した委託形式の情報とともに、コンテンツデータの分散処理が必要であるとデータ処理判断部41に通知する。

【0046】分散処理の委託形式には、一部の復号関連処理を委託する形式、または全ての復号関連処理を委託する形式などがある。一部の復号関連処理を委託する形式は、例えば、コンテンツデータにデジタル署名が付加されており、復号処理部43が、単独で復号処理とデジタル署名の検証処理を行ったのでは、要求されている時間内に処理を完了することができない場合に、一方の処理を委託する形式である。また、全ての復号関連処理を委託する形式は、復号処理部43が、コンテンツデータの暗号化アルゴリズムに対応していない場合に委託する形式である。なお、これらの委託形式は、データ送信装置21においてメタデータに記述することにより、または、データ受信装置23において予め設定することにより決定することが可能である。

【0047】ステップS21において、データ処理判断部42は、ステップS20で復号処理部43から通知された分散処理の委託形式などの情報に基づいて、コンテンツデータの分散処理先を検索する。分散処理先の候補は、データ処理判断部42にリスト化されて予め与えられている。

【0048】ステップS21の処理の結果、データ処理判断部42は、コンテンツデータの分散処理先として例えば計算部44を検出し、ステップS22において、計算部44に対して、コンテンツデータの分散処理を要求する。

【0049】ステップS23において、復号処理部43と、データ処理判断部42によりコンテンツデータの分散処理を要求された計算部44の間で、相互認証が行われる。この相互認証により、復号処理部43は、計算部44が分散処理した処理結果の出力先を指定する。復号処理部43は、計算部44に対して処理結果の出力先を例えば、データ記憶装置45と指定する。

【0050】ステップS24において、復号処理部43

は、計算部44と相互認証が成立したか否かを判定する。

【0051】ステップS24の処理の結果、復号処理部43が計算部44と相互認証が成立していないと判定した場合、復号処理部43は、コンテンツデータの復号関連処理が不可能であることを認識する。このとき、復号処理部43は、コンテンツデータの復号関連処理は不可能であることをデータ処理判断部42に通知する。その後、データ処理判断部42により処理は終了される。

【0052】ステップS24において、復号処理部43が、計算部44との相互認証が成立し、コンテンツデータの分散処理の準備が完了したと判定した場合、処理はステップS25に進む。

【0053】ステップS25において、復号処理部43からコンテンツデータの分散処理の準備が完了した旨の通知を受け取ったデータ処理判断部42は、データ送信装置21にコンテンツデータの送信を要求する。

【0054】ステップS26において、データ受信部41は、ネットワーク22を介してデータ送信装置21から送信されてくるコンテンツデータを受信する。

【0055】ステップS27において、データ受信部41が受信したコンテンツデータは、データ処理判断部42を経由して復号処理部43に転送され、復号処理部43は計算部44に対して、ステップS22でデータ処理判断部42が要求した委託形式に基づいて、コンテンツデータの分散処理を指令する。

【0056】ステップS28において、復号処理部43は、ステップS23で計算部44に通知した分散処理の出力先から、コンテンツデータの分散処理の結果を取得することができたか否かを判定する。復号処理部43は、分散処理の結果を取得することができないと判定した場合、ステップS29に進み、コンテンツデータは不正なデータであると認識し、データ処理判断部42に通知する。その後、データ処理判断部42は、データ受信装置23の利用者に対して不正があったことを通知するとともに、処理を終了する。

【0057】ステップS28において、復号処理部43は、計算部44に対して指定した出力先に、コンテンツデータの分散処理の結果が指定通りに転送されていると判定した場合、処理はステップS30に進む。

【0058】ステップS30において、復号処理部43による復号関連処理の結果は、計算部44による分散処理の処理結果とともに、データ記憶部45に記憶される。

【0059】図6は、本発明を適用したコンテンツ配信システムの構成を示す図である。コンテンツプロバイダ51は、コンテンツサーバ52を管理しており、コンテンツデータおよびメタデータを作成する。コンテンツプロバイダ51が作成したコンテンツデータおよびメタデータは、サービスプロバイダ53が管理するサービスサ

ーバ54に供給される。コンテンツデータは、映画、音楽などのデジタルデータであり、メタデータにはそれらのデータに関する情報が記述される。

【0060】サービスプロバイダ53は、ネットワーク22を介して、契約者である利用者55に対してコンテンツデータおよびメタデータを送信する。

【0061】利用者55は、サービスプロバイダ53から送信されたコンテンツデータおよびメタデータを、自らが操作する利用者端末56において利用する。

【0062】決済センタ57は、決済サーバ58を管理しており、利用者55に対してコンテンツデータの著作権情報を発行するとともに、著作権情報の代金の決済処理を行う。また、決済センタ57は、利用者55から支払われた代金を、コンテンツプロバイダ51と、サービスプロバイダ53の間で予め設定された契約に基づいて分配する。

【0063】図7は、コンテンツサーバ52の構成例を示すブロック図である。コンテンツサーバ52は、データキャプチャ装置71、データ編集装置72、メタデータ生成装置73、データ暗号化装置74、データ記憶装置75、およびデータ送信装置76より構成される。

【0064】データキャプチャ装置71は、外部から取り込んだデータを、コンテンツサーバ52の各装置が処理できるデータ形式に変換する。

【0065】データ編集装置72は、データキャプチャ装置71から転送されたデータから、利用者55に提供するコンテンツデータを作成する装置である。また、データ編集装置72は、メタデータ生成装置73が生成したメタデータをコンテンツデータに付加する。

【0066】データ暗号化装置74は、データ編集装置72から転送されたコンテンツデータおよびメタデータに暗号関連処理を施す。

【0067】データ記憶装置75は、データ暗号化装置74により暗号関連処理が施されたメタデータおよびコンテンツデータを記憶し、必要に応じてデータ送信装置76に転送する。

【0068】データ送信装置76は、サービスプロバイダ53が管理するサービスサーバ54にコンテンツデータを送信する。なお、具体的な各装置の処理については、図15のフローチャートを参照して後述する。

【0069】図8は、データ暗号化装置74の詳細な構成例を示すブロック図である。データ暗号化装置74は、入出力インタフェースブロック91、データ処理判断ブロック92、データ記憶ブロック93、乱数生成ブロック94、および暗号化処理ブロック95から構成される。さらに、暗号化処理ブロック95は、暗号化処理サブブロック96、デジタル署名生成サブブロック97、およびハッシュ値計算サブブロック98より構成される。

【0070】入出力インタフェースブロック91は、デ

ータ編集装置 72 から供給されるメタデータおよびコンテンツデータを、データ処理判断ブロック 92 に転送する。

【0071】データ処理判断ブロック 92 は、データ暗号化装置 74 の全体の動作を制御する。

【0072】データ記憶ブロック 93 は、暗号化処理ブロック 95 において、暗号関連処理が施されたメタデータおよびコンテンツデータや、処理に必要なデータを、適宜、記憶する。

【0073】乱数生成ブロック 94 は、データ処理判断ブロック 92 からの指令により乱数を生成し、暗号化処理ブロック 95 に供給する。乱数生成ブロック 94 が生成する乱数は、暗号化アルゴリズムである DES (Data Encryption Standard)、RSA (Rivest-Shamir-Adleman scheme) などの共通鍵暗号方式で暗号関連処理する場合の鍵として利用される。

【0074】暗号化処理ブロック 95 は、コンテンツデータの暗号化およびデジタル署名の生成処理を行う。この暗号化処理ブロック 95 の暗号化処理サブブロック 96 は、DES、RSA などの暗号化アルゴリズムによりコンテンツデータの暗号化処理を行う。

【0075】デジタル署名生成サブブロック 97 は、DSA (Digital Signature Algorithm) などによるデジタル署名の生成アルゴリズムによりデジタル署名を生成する。デジタル署名は、データの改竄のチェックおよびデータの制作者を認証するためのデータである。

【0076】ハッシュ値計算サブブロック 98 は、ハッシュ関数による計算を行う。ハッシュ関数は、送信するデータを入力とし、所定のビット長のデータに圧縮し、ハッシュ値として出力する関数である。ハッシュ関数は、出力であるハッシュ値から入力データを復元することが難しく、また、同一の出力結果のハッシュ値を持つ入力データを探し出すことが困難である（一方向である）特徴を有する。

【0077】ここで、デジタル署名の生成および検証について説明する。デジタル署名の生成者は、送信するデータから特定のアルゴリズムを用いて、メッセージダイジェストを作成する（ハッシュ値計算サブブロック 98 により、送信するデータに、ハッシュ関数を適用し、メッセージダイジェストを作成する）。デジタル署名の生成者は、自分の秘密鍵（乱数生成ブロック 94 により生成された乱数）を使って、このメッセージダイジェストと送信するデータの全文を暗号化し、利用者に送信する。

【0078】一方、データの利用者は、データを受信し、デジタル署名の生成者が提供する公開鍵を利用して、暗号化されているデータの全文、およびメッセージダイジェストを復号処理する。次に、データの利用者は復号したデータの全文から、デジタル署名の生成者と同じ方式（同一のハッシュ関数）でメッセージダイ

ジェストを作成する。生成されたメッセージダイジェストと受信されたメッセージダイジェストを比較することにより、デジタル署名の検証が行なわれる。すなわち、データの送信者から送信され、受信者が復号したメッセージダイジェストと、受信者が復号したデータの全文から、送信者と同じ方式により作成したメッセージダイジェストが等しければ、そのデータは改竄などの不正な処理が行われていないことを表す。

【0079】なお、データ暗号化装置 74 において、説明の便宜上、暗号化処理サブブロック 96、およびデジタル署名生成サブブロック 97 は暗号関連処理を行うことが可能であるとしたが、通常は、復号関連処理も行うことが可能である。すなわち、暗号化処理サブブロック 96 はデータの暗号化および復号が可能であるし、デジタル署名生成サブブロック 97 はデジタル署名の生成および検証が可能である。

【0080】さらに、後述する図 13 の暗号化処理ブロック 163 に配置されている暗号化処理部 186 を構成するサブブロックも、データ暗号化装置 74 を構成するサブブロックと同様に、復号関連処理だけでなく暗号関連処理を実行することができる。また、サービスサーバ 54 に配置されているデータ暗号化装置 114 も上述したコンテンツサーバ 52 に配置されているデータ暗号化装置 74、および復号処理ブロック 163 と同様に、復号関連処理だけでなく暗号関連処理を実行することができる。これにより、それぞれの装置間で送受信されるデータに、改竄などの不正な処理が行われることを防ぐことが可能となる。

【0081】上述したような暗号関連処理が施されたコンテンツデータおよびメタデータは、サービスプロバイダ 53 が管理するサービスサーバ 54 に送信される。

【0082】図 9 は、サービスサーバ 54 の構成例を示すブロック図である。サービスサーバ 54 は、データ送受信装置 111、データ編集装置 112、メタデータ生成装置 113、データ暗号化装置 114、コンテンツプロモーションサーバ 115、およびデータ記憶装置 116 より構成される。

【0083】データ送受信装置 111 は、コンテンツサーバ 52 から送信されるコンテンツデータおよびメタデータを受信する。また、データ送受信装置 111 は、利用端末 56 に対し、ネットワーク 22 を介してコンテンツデータおよびメタデータを送信する。データ送受信装置 111 は、コンテンツデータおよびメタデータを送信するタイミングを判断する。送信するタイミングは、例えば、利用者 55 からの要求に応じて送信する場合や、メタデータに記述されているタイミングで送信する場合などがある。

【0084】データ編集装置 112 は、サービスサーバ 54 の各装置で処理されたデータを編集し、利用者 55 に提供する形態にデータを編集する。



【0085】メタデータ生成装置113は、メタデータを生成する。メタデータ生成装置113が生成するメタデータには、サービスプロバイダ53がコンテンツデータを利用者55に提供する際に、サービスプロバイダ53が利用者55に対して通知する情報が記述される。

【0086】データ暗号化装置114は、メタデータ生成装置113が生成したメタデータにデジタル署名を生成するなどの暗号関連処理を行う。データ暗号化装置114の詳細な構成は、図7に示すコンテンツサーバ52のデータ暗号化装置74（図8）の構成と同様である。

【0087】コンテンツプロモーションサーバ115は、サービスプロバイダ53が利用者55に提供するコンテンツの一覧情報を作成するとともに、ディスカウント情報などを利用者55の要求に応じて提供する。コンテンツプロモーションサーバ115は、WWWサーバとして設置され、利用者55は利用者端末56に装備されているブラウザを利用することにより、コンテンツプロモーションサーバ115が提供するサービスを受けることができる。さらに、コンテンツプロモーションサーバ115は、利用者55からの電話による問い合わせに対応できるようにもなっている。

【0088】データ記憶装置116は、データ編集装置112で編集されたデータを記憶し、利用者55からの要求に応じて、データ送受信装置111に対してコンテンツデータおよびメタデータを転送する。なお、具体的な各装置の処理については、図18のフローチャートを参照して後述する。

【0089】図10は、決済センタ57が管理している決済サーバ58の構成例を示すブロック図である。決済サーバ58は、データ送受信装置131、ライセンス装置132、ユーザ管理装置133、著作権管理装置134、課金装置135、および決済装置136より構成される。

【0090】データ送受信装置131は、利用者端末56から、ネットワーク22を介して通知されるコンテンツデータの著作権の購入要求情報を受信するとともに、コンテンツプロバイダ51およびサービスプロバイダ53に対して、利用者55から回収した代金の課金情報を送信する。

【0091】ライセンス装置132は、利用者55からコンテンツデータの著作権購入が要求された場合、著作権情報の発行処理を行う。

【0092】ユーザ管理装置133は、サービスプロバイダ53から、コンテンツデータの提供を受ける契約をしている利用者55、およびその利用者55が操作する利用者端末56の情報を管理する。利用者55および利用者端末56の情報には、利用者端末56に含まれるセットトップボックスの契約日、契約条件、サービスの利用情報などが含まれる。

【0093】著作権管理装置134は、コンテンツデータの著作権の他、サービスプロバイダ53から提供される利用者55が利用可能なコンテンツデータの利用形態、および利用者55によるコンテンツデータの購入履歴などを管理する。

【0094】課金装置135は、コンテンツデータの著作権情報の料金情報を管理するとともに、利用者55に対して、課金情報を通知する。

【0095】決済装置136は、課金装置135から決済処理の要求をうけて、決済処理を行う。具体的な決済方法には、クレジットカードによる決済方法、プリペイド型の電子マネーによる決済方法が含まれる。なお、決済サーバ58の使用権情報の発行処理については、図20および21のフローチャートを参照して後述する。

【0096】図11は、利用者55が管理する利用者端末56の構成例を示すブロック図である。利用者端末56は、セットトップボックス151（以下、適宜、STB151と称する）、およびデータ再生装置152より構成される。

【0097】STB151は、ネットワーク22を介して、サービスサーバ54、および決済サーバ58との間でデータの送受信を行う。STB151の詳細な構成例は図12に示す。

【0098】データ再生装置152は、サービスサーバ54から提供され、STB151が処理したコンテンツデータを再生する装置である。データ再生装置152は、例えば、テレビジョン受像機、パーソナルコンピュータなどの電子機器により構成される。

【0099】図12は、セットトップボックス151の構成例を示すブロック図である。STB151は、データ送受信ブロック161、コントローラ162、暗号化処理ブロック163、フラッシュメモリ164、および外部RAM（Random Access Memory）165から構成される。

【0100】データ送受信ブロック161は、サービスサーバ54から、ネットワーク22を介して送信されるコンテンツデータおよびメタデータ、若しくは決済サーバ58から送信されるコンテンツデータの著作権情報などを受信する。また、データ送受信ブロック161は、サービスサーバ54に対するデータの送信要求、および決済サーバ58に対する著作権情報を要求する情報などを送信するとともに、データ再生装置152に、処理結果を転送する。

【0101】コントローラ162は、ソフトウェアにより制御され、STB151全体の動作を制御する。

【0102】暗号化処理ブロック163は、データ送受信ブロック161が受信するコンテンツデータおよびメタデータの復号関連処理を行う。詳細な構成例については図13に示す。

【0103】フラッシュメモリ164は、STB151の

電源遮断後もデータを記憶している不揮発性のメモリである。フラッシュメモリ164には、各ブロックが処理するために必要なデータ、および各ブロックの処理結果が、適宜、記憶される。

【0104】外部RAM165は、暗号化処理ブロック163による処理結果、および他のブロックが分散処理を行った場合の分散処理結果を記憶する。

【0105】図13は、暗号化処理ブロック163の詳細な構成例を示すブロック図である。暗号化処理ブロック163は、入出力インタフェースブロック181、マイクロプロセッサ182、RAM183、乱数生成ブロック184、フラッシュメモリ185、および暗号化処理部186より構成される。さらに、暗号化処理部186は、暗号化処理サブブロック187、デジタル署名検証サブブロック188、およびハッシュ値計算サブブロック189より構成される。

【0106】入出力インタフェースブロック181は、データ送受信ブロック161が受信したコンテンツデータおよびメタデータのうち、コントローラ162により復号関連処理が必要であると判断され、暗号化処理ブロック163に転送されるデータを受信する。入出力インタフェースブロック181は、コントローラ161から供給されるデータを、マイクロプロセッサ182に転送する。マイクロプロセッサ182は、暗号化処理ブロック163の全体の動作を制御する。

【0107】RAM183は、マイクロプロセッサ182が処理をするのに必要なプログラムを記憶している。また、RAM183には、マイクロプロセッサ182が処理した結果が記憶される。

【0108】乱数生成ブロック184は、マイクロプロセッサ182からの指令により乱数を生成し、暗号化処理部186に供給する。乱数生成ブロック184が生成した乱数は、DES、RSAなどの共通鍵暗号方式で暗号関連処理が施されたデータを、復号する場合の鍵として利用される。

【0109】フラッシュメモリ185は、不揮発性のメモリであり、内部に図示せぬコントローラを保持している。マイクロプロセッサ182において動作するソフトウェアの実行コード、復号関連処理に必要となる各種データ、購入したコンテンツデータの著作権情報などが記憶される。

【0110】暗号化処理部186は、コンテンツデータおよびメタデータの復号関連処理を行う。暗号化処理部186は、さらに、以下の機能を提供するサブブロックにより構成される。

【0111】暗号化処理サブブロック187は、DES、RSAなどの暗号化アルゴリズムにより暗号化されたコンテンツデータの復号処理を行う。

【0112】デジタル署名検証サブブロック188は、DSAなどによるデジタル署名アルゴリズムにより

デジタル署名が付加されたコンテンツデータおよびメタデータのデジタル署名検証処理を行う。

【0113】ハッシュ値計算サブブロック189は、ハッシュ関数による計算を行う。

【0114】図14は、暗号化処理ブロック163が、コントローラ162等と送受信するデータ形式の例を示す図である。コントローラ162は、暗号化処理ブロック163に対して、図14のデータ形式のコマンドデータで処理を要求する。また、暗号化処理ブロック163は、コマンドデータに基づいて各ブロックを制御し、所定の処理を実行させるとともに、コマンドデータにより処理を要求したコントローラ162に対して、図14のデータ形式のレスポンスデータで処理結果を送信する。

【0115】フィールド1は、データ種識別フィールドであり、コマンドデータ、またはレスポンスデータの種類の記述される。

【0116】フィールド2は、データ番号フィールドであり、コマンドデータ、またはレスポンスデータの番号が記述される。

【0117】フィールド3は、データ長フィールドであり、データフィールド4に記述されるデータの長さが記述される。

【0118】フィールド4は、データフィールドであり、コマンドデータとして処理を要求するデータ、またはレスポンスデータとして送信する処理結果のデータが記述される。以下、コマンドデータ、およびレスポンスデータの例を説明する。

【0119】データ番号フィールドに記述される番号が1であるコマンド1は、デジタル署名の検証処理の要求を表している。フィールド4のデータフィールドに記述されているデータに対して、暗号化処理ブロック163は、データが改竄されていないかを検証し、その処理結果をレスポンス1として、データ処理を要求したブロックに送信する。

【0120】コマンド2は、デジタル署名の生成処理の要求を表している。暗号化処理ブロック163は、フィールド4のデータフィールドに記述されているデータに対して、デジタル署名を付加したデータをレスポンス2として、データ処理を要求したブロックに送信する。

【0121】コマンド3は、暗号化されているデータの復号処理の要求を表している。暗号化処理ブロック163は、フィールド4のデータフィールドに記述されている暗号化されているデータに対して、復号処理を行い、復号したデータをレスポンス3として、データ処理を要求したブロックに送信する。

【0122】コマンド4は、暗号化処理の要求を表している。暗号化処理ブロック163は、フィールド4のデータフィールドに記述されているデータを暗号化し、暗号化したデータをレスポンス4として、データ処理を要

求したブロックに送信する。

【0123】コマンド5は、ハッシュ値計算の要求を表している。ハッシュ値計算サブブロック189は、フィールド4のデータフィールドに記述されているデータ、およびアルゴリズムをもとに、ハッシュ関数による計算を行い、計算結果のデータをレスポンス5として、データ処理を要求したブロックに送信する。

【0124】コマンド6は、処理の停止要求を表している。このコマンドを受信した場合、暗号化処理ブロック163は、その時点で実行している処理を停止し、停止した旨の通知をレスポンス6として処理の停止を要求するブロックに送信する。

【0125】コマンド7は、使用権情報の送信要求を表している。このコマンドを受信した場合、暗号化処理ブロック163は、自らがフラッシュメモリ185に保持している使用権情報を暗号化して、決済サーバ58にレスポンス7として送信する。

【0126】コマンド20は、外部装置または他のブロックから送信されるメッセージである。そのデータフィールドには、コンテンツデータの分散処理先である装置、コントローラ162などからメッセージが入力される。

【0127】レスポンス30は、暗号化処理ブロック163が、外部装置または他のブロックに対して送信するメッセージである。

【0128】以下、コンテンツプロバイダ51が提供するコンテンツデータを、利用者55が利用するまでの一連の処理についてフローチャートを参照して説明する。

【0129】始めに、図15のフローチャートを参照して、コンテンツプロバイダ51が管理するコンテンツサーバ52の処理を説明する。

【0130】ステップS41において、データキャプチャ装置71は、ビデオカメラ、およびオーディオレコーダなどから取り込んだアナログデータ、またはデジタルデータを、コンテンツサーバ52の各装置が処理できるデータ形式に、デジタル化処理、または圧縮などの処理を行う。

【0131】ステップS42において、データ編集装置72は、データキャプチャ装置71から取得したデータから、コンテンツプロバイダ51の指令に基づいて、利用者55に提供するコンテンツデータを作成する。また、データ編集装置72は、メタデータ生成装置73が生成するメタデータをコンテンツデータに付加する。

【0132】図16は、メタデータ生成装置73が生成するメタデータの例を示す図である。図16(A)のメタデータ1の例において、フィールド1には、コンテンツプロバイダ51を特定するコンテンツプロバイダIDが2、メタデータ1に対応するコンテンツデータ（以下、適宜、コンテンツデータ1と称する。後述する他のメタデータが付加されるコンテンツデータの場合も同様とす

る）を特定するコンテンツIDが1、コンテンツデータ1の著作権の権利発生日時が西暦2000年1月1日と記述されている。

【0133】フィールド2には、利用者55によるコンテンツデータ1の利用形態が記述される。ここでは、利用形態1としてストリーミング、利用形態2として買い取りが記述されている。ストリーミングによる利用形態は、利用者端末56において、サービスサーバ54からコンテンツデータ1を受信しながらリアルタイムで再生する利用形態であり、利用回数が1回のみ利用形態である。買い取りによる利用形態とは、期間および利用回数が無制限である利用形態であり、利用者端末56に送信されたコンテンツデータ1は、利用者端末56の図示せぬ記録媒体に記録される。

【0134】フィールド3には、コンテンツデータ1の利用形態毎の料金が記述される。ここでは、コンテンツデータ1を利用形態1のストリーミングにより利用した場合、料金は20円とされ、コンテンツデータ1を利用形態2の買い取りにより利用した場合、料金は100円とされている。利用者55は、フィールド3に記述される料金に基づいて、決済センタ57に対して使用権情報の代金を支払う。

【0135】フィールド4には、コンテンツデータ1の形式的な情報が記述される。ここでは、コンテンツデータ1の総データ量は57.6MBで、利用者端末56のデータ再生装置152で再生した場合の再生時間は10分と記述されている。また、コンテンツデータ1は、MP3(MPEG(Moving Picture Experts Group)-1 Audio Layer 3)の規格で圧縮されているオーディオデータであり、データ転送速度は128Kbpsと記述されている。

【0136】フィールド5には、データ暗号化装置74がコンテンツデータおよびメタデータに施した暗号関連処理の情報が記述される。この例で、デジタル署名の生成アルゴリズムはDSA、コンテンツデータ1の暗号化アルゴリズムはDES、コンテンツデータ1の暗号化のデータ単位は64KBと記述されている。暗号化のデータ単位は、1つの暗号化の鍵で連続して暗号化する場合のデータの大きさである。暗号化に利用した鍵はさらに別の鍵(メタ鍵)で暗号化されており、メタ鍵は決済センタ57に委託され、利用者55が使用権情報を購入した場合、決済サーバ58から使用権情報とともに、後述する図22の使用権情報のデータ形式で、利用者55に提供される。

【0137】図16(B)のメタデータ2の例において、フィールド1には、コンテンツプロバイダIDが2、コンテンツIDが2、著作権の権利発生日時が西暦2000年1月1日として記述されている。

【0138】フィールド2には、コンテンツデータ2の利用形態1としてストリーミング、利用形態2として買い取り、利用形態3として期間限定1年が記述されてい

る。期間限定1年の利用形態とは、コンテンツデータ2が利用者端末56の図示せぬ記録媒体に記録された後、利用者55は期間が1年間以内であれば、回数は無制限にコンテンツデータ2を利用することが可能な形態である。

【0139】フィールド3には、コンテンツデータ2の料金が記述されている。料金は、利用形態1のストリーミングにより利用した場合は20円とされ、利用形態2の買い取りによる利用の場合は100円とされ、利用形態3の期間限定1年による利用の場合は50円とされている。

【0140】フィールド4には、コンテンツデータ2の総データ量は300MB、再生時間は10分と記述されている。また、コンテンツデータ2は、MPEG-2の規格で圧縮されているビデオデータであり、データの転送速度は4Mbpsである。

【0141】フィールド5には、デジタル署名の生成アルゴリズムはDSA、コンテンツデータの暗号化アルゴリズムはDES、暗号化のデータ単位は256KBと記述されている。

【0142】図15に戻って、ステップS43において、データ暗号化装置74は、データ編集装置72から転送されるコンテンツデータおよびメタデータに暗号関連処理を施す。

【0143】すなわち、乱数生成ブロック94は、暗号化鍵（コンテンツデータ用）として所定のビット数の乱数を生成し、暗号化処理サブブロック96に供給する。

【0144】暗号化処理サブブロック96は、乱数生成ブロック94が生成した乱数を暗号鍵としてコンテンツデータを暗号化するとともに、使用権情報に配置されて決済サーバ58から利用者端末56に対して送信されるメタ鍵を使用して、暗号化鍵（コンテンツデータ用）をDESなどの共通鍵暗号方式で暗号化する。

【0145】ハッシュ値計算サブブロック98は、コンテンツサーバ52がサービスプロバイダ53に対して送信するメタデータにハッシュ関数を適用してハッシュ値を算出する。

【0146】デジタル署名生成サブブロック97は、ハッシュ値計算サブブロック98が抽出したハッシュ値を、乱数生成ブロック94が生成した乱数よりなる暗号化鍵を利用して暗号化し、デジタル署名を生成する。

【0147】ステップS44において、データ記憶装置75は、データ暗号化装置74により暗号関連処理が施されたデータを記憶し、必要に応じてデータ送信装置76に出力する。

【0148】ステップS45において、データ送信装置76は、サービスプロバイダ53が管理するサービスサーバ54にメタデータおよびコンテンツデータを送信する。

【0149】図17は、ステップS45の処理により送

信されるデータのフォーマットの例を示す。レイヤ1は、ステップS42の処理により生成されたメタデータ、ステップS43の処理により付加されたメタデータ用のデジタル署名、ステップS43の処理で用いられた暗号化鍵（コンテンツデータ用）、並びにコンテンツデータにより構成される。コンテンツデータは、さらに、レイヤ2としての暗号化単位ブロックにより構成されている。暗号化単位ブロックは、コンテンツデータ1の場合64KB毎のブロックとされ、コンテンツデータ2の場合256KB毎のブロックとされている。

【0150】次に、図18のフローチャートを参照して、サービスプロバイダ53が管理するサービスサーバ54の処理を説明する。

【0151】ステップS61において、データ送受信装置111は、コンテンツサーバ52から、暗号関連処理が施されたコンテンツデータおよびメタデータを受信する。

【0152】ステップS62において、メタデータ生成装置113は、送信されてきたメタデータを確認し、元のデータを変更し、新たなメタデータを生成する。すなわち、このときデータ暗号化装置114は、コンテンツプロバイダ51から決済サーバ58を介して予め取得したメタ鍵を利用して、送信されてきた暗号化鍵（コンテンツデータ用）（図17）を復号し、復号した暗号化鍵（コンテンツデータ用）（図17）を利用してデジタル署名（メタデータ用）（図17）を復号する。そして、メタデータ生成装置113は、復号して得られたメタデータと、平文で送信されてきたメタデータを比較し、両者が一致していること、すなわち、メタデータが改竄されていないことを確認する。

【0153】さらに、メタデータ生成装置113は新たにメタデータを生成する。このメタデータは、コンテンツサーバ52が生成したメタデータ1（図16（A））およびメタデータ2（図16（B））のフィールド1およびフィールド3の内容を、サービスプロバイダ53が利用者55に通知する情報に書き換えたデータである。メタデータ3およびメタデータ4の内容は、サービスプロバイダ53が決定する。

【0154】図19は、図16に示されるコンテンツプロバイダ51が生成したメタデータを、ステップS62の処理で、メタデータ生成装置113が変更して生成したメタデータの例を示す。図16（A）のメタデータ1を変更して生成されたメタデータ3（図19（A））の例においては、フィールド1には、サービスプロバイダ53を特定するサービスプロバイダIDが2、メタデータ3を作成した日時が西暦2000年1月2日と記述されている。

【0155】フィールド3に記述されている料金には、図16（A）に示すメタデータ1のフィールド3に記述されている料金に、サービスプロバイダ53が利用者5

5に対してコンテンツデータを送信する送信料が付加されている。メタデータ3では、料金は、コンテンツデータをストリーミングの利用形態により利用する場合は、コンテンツプロバイダ51が受け取るコンテンツデータの料金に、サービスプロバイダ53が受け取る送信料の10円が付加されて30円とされ、コンテンツデータを買取りの利用形態により利用する場合は、コンテンツプロバイダ51が受け取るコンテンツデータの料金に、サービスプロバイダ53が受け取る送信料の50円が付加されて150円とされている。

【0156】図16(B)のメタデータ2を変更して生成された図19(B)のメタデータ4の例においては、フィールド1には、サービスプロバイダIDが2、メタデータ4を作成した日時が西暦2000年1月2日と記述されている。

【0157】フィールド3に記述される料金には、コンテンツデータの利用形態がストリーミングの場合は、コンテンツプロバイダ51が受け取るコンテンツデータの料金に、送信料の10円が付加されて30円とされ、利用形態が買取りの場合は、送信料の50円が付加されて150円とされ、さらに利用形態が期間限定1年の場合は送信料の30円が付加されて80円とされている。

【0158】ステップS63において、データ暗号化装置114は、新たに生成したメタデータのハッシュ値を演算し、それを暗号化鍵（コンテンツデータ用）で暗号化し、新たなデジタル署名を生成し、ステップS62の処理で生成された新たなメタデータに付加する。データ暗号化装置114の暗号関連処理は、コンテンツサーバ52のデータ暗号化装置74の処理と同様に行われる。

【0159】ステップS64において、データ編集装置112は、サービスサーバ54の各装置で処理されたデータを編集し、利用者55に提供するコンテンツデータを作成する。このため、暗号化装置114は、送信されてきたコンテンツデータを暗号化鍵（コンテンツデータ用）で一旦復号する。その後データ編集装置112により行われる編集には、コンテンツサーバ52から送信されたコンテンツデータにステップS62の処理で生成されたメタデータを付加する処理、または複数のコンテンツデータを統合し、1つのコンテンツデータにまとめて利用者55に提供するアルバム化などの処理がある。編集後のコンテンツデータは、データ暗号化装置114により暗号化鍵（コンテンツデータ用）を用いて再び暗号化される。

【0160】ステップS65において、データ記憶装置116は、データ編集装置112で編集され、データ暗号化装置114により暗号化されたデータを記憶する。

【0161】ステップS66において、データ送受信装置111は、利用者55が管理する利用者端末56から、メタデータの送信が要求されたか否かを判定し、メ

タデータの送信が要求されたと判定するまで待機する。その後、データ送受信装置111が、メタデータの送信が要求されたと判定した場合、処理はステップS67に進む。

【0162】ステップS67において、データ送受信装置111は、利用者55が要求するコンテンツデータに対応するメタデータを、データ記憶装置116から取得し、ネットワーク22を介して利用者端末56に送信する。データ送受信装置111が送信するメタデータを受信した利用者端末56のSTB151は、メタデータに記述されている内容を確認し、コンテンツデータの復号関連処理の準備をする。STB151の詳細な処理については後述するが、その後、STB151からコンテンツデータの送信が要求されてくる。

【0163】そこで、ステップS68において、データ送受信装置111は、利用者端末56からコンテンツデータの送信が要求されたか否かを判定する。

【0164】データ送受信装置111が、利用者端末56からコンテンツデータの送信が要求されたと判定した場合、処理はステップS69に進み、データ送受信装置111は、データ記憶装置116に記憶されているコンテンツデータを、ネットワーク22を介して利用者端末56に送信する。

【0165】次に、決済センタ57が管理する決済サーバ58が、利用者端末56に対して行うコンテンツデータの使用権情報の発行処理について、図20および図21のフローチャートを参照して説明する。

【0166】ステップS81において、ライセンス装置132は、利用者端末56からコンテンツデータの使用権情報の購入が要求されたか否かを判定し、要求されたと判定するまで待機する。ライセンス装置132が、利用者端末56から使用権情報の購入が要求されたと判定した場合、処理はステップS82に進む。

【0167】ステップS82において、ライセンス装置132は、使用権情報の購入を要求している利用者55は、サービスプロバイダ53からコンテンツデータの提供を受ける契約をしているか否かを確認するため、利用者端末56のSTB151から送信される情報に基づいて、STB151は契約対象の機器であるか否かをユーザ管理装置133に問い合わせる。この問い合わせに応じて、ユーザ管理装置133は、自分自身が管理している契約情報から、使用権情報の購入を要求するSTB151は、契約対象の機器であるか否かを検索する。すなわち、このシステムでは、利用者55はコンテンツデータの提供を受ける前に、サービスプロバイダ53と予め契約をする必要がある。契約情報は、サービスプロバイダ53から決済センタ57に供給され、ユーザ管理装置133に登録される。

【0168】ステップS83において、ライセンス装置132は、ステップS82のユーザ管理装置133の検

索結果を判定する。ライセンス装置132は、使用権情報の購入を要求しているSTB151は、契約対象の機器でないと判定した場合、利用者端末56に対して使用権情報を販売することができないことを通知し、処理を終了する。

【0169】ライセンス装置132が、使用権情報の購入を要求しているSTB151は、契約対象の機器であると判定した場合、処理はステップS84に進み、ライセンス装置132は、データ送受信装置131からネットワーク22を介してSTB151の暗号化処理ブロック163と相互認証を行い、セッション鍵を共有する。

【0170】ステップS85において、ライセンス装置132は、相互認証が成立したか否かを判定し、相互認証が成立していないと判定した場合、処理を終了する。

【0171】ステップS85において、ライセンス装置132が、相互認証が成立したと判定した場合、処理はステップS86に進み、ライセンス装置132は、STB151から送信される要求内容に基づいて、使用権情報の発行が可能であるか否かを著作権管理装置134に問い合わせる。STB151から送信される要求内容には、利用者55が利用を希望するコンテンツデータのコンテンツID、コンテンツデータの利用形態、および使用権情報の代金の決済方法が含まれる。(決済方法がクレジットカードによる決済の場合、クレジットカードのカード番号が、また、決済方法がプリペイドカード型の電子マネーによる決済の場合、プリペイドカードのカード番号が、それぞれ含まれる)このSTB151から送信される要求情報は、改竄などの不正処理を防ぐため、暗号化処理ブロック163により暗号化されてSTB151から送信される。

【0172】ステップS87において、ライセンス装置132は、ステップS86で著作権管理装置134に問い合わせた結果を判定する。ライセンス装置132は、使用権情報の発行ができないと判定した場合、利用者端末56に使用権情報の発行ができないことを通知し、処理を終了する。

【0173】ステップS87において、ライセンス装置132が、使用権情報の発行が可能であると判定した場合、処理はステップS88に進み、ライセンス装置132は、課金装置135に対して課金処理を要求する。

【0174】ステップS89において、課金装置135は、自らが管理している料金情報から、利用者55が要求する使用権情報の代金を取得し、決済装置136に対して決済処理の要求をするとともに、利用者端末56に対して課金情報を通知する。

【0175】ステップS90において、課金装置135から決済処理の要求を受けた決済装置136は決済処理を行う。決済方法がクレジットカードによる決済の場合、決済装置136は、図示せぬクレジットカード会社の決済サーバに、使用権情報の購入を要求している利用

者55のユーザID、および課金装置135が取得した使用権情報の代金を通知し、クレジット会社の決済サーバから、決済が可能であるか否かのメッセージを受け取る。決済装置136は、メッセージの結果を課金装置135に通知する。

【0176】利用者55が要求する決済方法が、プリペイドカード型の電子マネーによる決済の場合、決済装置136は、利用者55から通知されたカードIDと、自身自身が管理するプリペイドカードのカードIDを照合し、決済が可能であるか否かを判定する。決済装置136は、この判定結果を課金装置135に通知するとともに、決済が可能である場合、利用者55が使用しているプリペイドカード型の電子マネーの残高情報を更新する。

【0177】ステップS91において、課金装置135は、決済装置136から通知される情報により、決済が成立したか否かを判定する。決済が成立していないと判定した場合、課金装置135は、決済が成立していないことを利用者55に通知し、処理を終了する。

【0178】ステップS91において、課金装置135は、決済が成立したと判定した場合、ライセンス装置132に決済が成立したことを通知する。

【0179】このときステップS92において、ライセンス装置132は、使用権情報をセッション鍵で暗号化し、ネットワーク22を介して利用者端末56に送信する。送信された使用権情報は、STB151の暗号化処理ブロック163によりセッション鍵で復号される。

【0180】図22は、使用権情報の例を示している。この使用権情報の例では、フィールド1には、利用者55に対してコンテンツデータの使用権情報の発行を許可するコンテンツプロバイダ51のIDが2、利用が許可されたコンテンツデータのコンテンツIDが1、および使用権の権利発生日時が西暦2000年1月2日と記述されている。

【0181】フィールド2にはコンテンツプロバイダ51により許可された利用形態がストリーミングであることが記述されており、フィールド3には、そのストリーミングによる利用形態の料金が30円とされている。

【0182】フィールド4には、メタ鍵が配置されている。通常、利用が許可されたコンテンツデータを復号するための鍵(暗号化鍵(コンテンツデータ用)(図17))は暗号化されており、メタ鍵はその暗号化鍵(コンテンツデータ用)を復号して取得するための鍵である。

【0183】フィールド5には、使用権情報全体のデジタル署名が付加される。

【0184】使用権情報は、STB151の暗号化処理ブロック163により、そのデジタル署名の検証が行われた後、暗号化処理ブロック163の内部に配置されているフラッシュメモリ185に記憶される。記憶された

使用権情報は、コンテンツデータの復号関連処理において、適宜、利用される。

【0185】次に、使用権情報を取得した後のSTB151の処理について、図23乃至図25のフローチャートを参照して説明する。

【0186】ステップS101において、利用者55からの指令に基づいてSTB151のコントローラ162は、サービスサーバ54に対して、使用権情報を購入したコンテンツデータに対応するメタデータの送信を要求する。

【0187】ステップS102において、データ送受信ブロック161は、サービスサーバ54から送信されたメタデータを、ネットワーク22を介して受信する。

【0188】ステップS102で受信されたメタデータは、図19に示すメタデータ3またはメタデータ4である。コントローラ162は、メタデータにはデジタル署名が付加されているため、デジタル署名の検証が必要であると認識する。そこで、コントローラ162は、メタデータを暗号化処理ブロック163に転送する。

【0189】ステップS103において、暗号化処理ブロック163のマイクロプロセッサ182は、転送されてきたメタデータのデジタル署名を検証し、メタデータの正当性を判断する。

【0190】すなわち、ハッシュ値計算サブブロック189は、平文で送られてきたメタデータにハッシュ関数を適用してハッシュ値を演算する。暗号化処理サブブロック187は、フラッシュメモリ185に記憶されているメタ鍵で暗号化鍵（コンテンツデータ用）を復号し、さらに、暗号化鍵（コンテンツデータ用）でデジタル署名を復号し、そこに含まれるハッシュ値を得る。デジタル署名検証サブブロック188は、ハッシュ値計算サブブロック189が、転送されたメタデータの全文からハッシュ関数を利用して算出したハッシュ値と、暗号化処理サブブロック187により復号されたハッシュ値を比較することにより、デジタル署名を検証する。なお、ハッシュ値計算サブブロック189が利用するハッシュ関数は、コンテンツサーバ52のハッシュ値計算サブブロック98や、サービスサーバ54のデータ暗号化装置114が利用するハッシュ関数と同一の関数である。

【0191】マイクロプロセッサ182は、デジタル署名検証サブブロック188が検証した結果を取得し、不正処理の有無を判定する。

【0192】ステップS104において、マイクロプロセッサ182は、メタデータが正常なデータ（改竄されていないデータ）であるか否かを判定し、不正処理を認識した場合（ハッシュ値が一致しない場合）、コントローラ162に通知する。コントローラ162は、不正処理の存在を利用者55に通知し、処理を終了する。

【0193】ステップS104において、マイクロプロ

セッサ182により、メタデータが正常なデータであることが確認された場合、処理はステップS105に進み、マイクロプロセッサ182は、受信したメタデータの内容を、決済センタ57から購入し、フラッシュメモリ185に記憶されている使用権情報の内容と比較する。これにより、データ送受信ブロック161が受信したメタデータは、利用者55が使用権情報を購入し、サービスサーバ54に送信を要求するコンテンツデータに対応するメタデータであるか否かがマイクロプロセッサ182により判定される。

【0194】ステップS106において、ステップS105でマイクロプロセッサ182が比較した結果が、マイクロプロセッサ182により判定される。マイクロプロセッサ182は、メタデータの内容が、使用権情報の内容と一致せず、正当性が確認できないと判定した場合、コントローラ162に通知する。コントローラ162は、利用者55に対してメタデータに不正処理が存在していることを通知し、処理を終了する。

【0195】ステップS106において、マイクロプロセッサ182が、メタデータの内容と使用権情報の内容を比較し、メタデータの正当性を確認した場合、処理はステップS107に進む。マイクロプロセッサ182は、メタデータに含まれる暗号関連処理情報を確認し、自分自身の復号関連処理の処理能力と比較することにより、コンテンツデータの復号関連処理の準備をする。この例の暗号化処理ブロック163は、DESのアルゴリズムで暗号化されているコンテンツデータを復号する機能を有しており、復号関連処理の結果を出力する転送速度は、3Mbpsであるとする。暗号化処理ブロック163のこれらの処理能力を基準に、分散処理が必要であるか否かが、ステップS108において、マイクロプロセッサ182により判定される。

【0196】例えば、サービスサーバ54から送信されるコンテンツデータに、図19(A)のメタデータ3が対応されている場合のマイクロプロセッサ182の処理について説明する。

【0197】マイクロプロセッサ182は、メタデータ3の内容から、暗号化されているコンテンツデータ3を復号するには、DESのアルゴリズムに対応していることが必要であり、MP3の規格で圧縮されたオーディオデータを、ストリーミングにより再生するには、128Kbpsの転送速度の処理能力が要求されていると認識する。ここでマイクロプロセッサ182は、自分自身の処理能力と、要求されている処理能力を比較することにより、単独で、コンテンツデータ3を処理することが可能であると判定する。この場合、ステップS108において、マイクロプロセッサ182は、分散処理が必要でないと判定し、処理はステップS109に進む。

【0198】ステップS109において、マイクロプロセッサ182から、暗号化処理ブロック163が、単独

10

20

30

40

50

でコンテンツデータ3の処理をすることが可能であると通知を受けたコントローラ162は、サービスサーバ54に対してコンテンツデータ3の送信を要求する。

【0199】ステップS110において、ステップS109でコントローラ162が要求するコンテンツデータ3は、サービスサーバ54から送信され、ネットワーク22を介してデータ送受信ブロック161により受信される。コントローラ162からコンテンツデータ3の転送を受けた暗号化処理ブロック163は、単独で、コンテンツデータ3を復号する。

【0200】すなわち、暗号化処理ブロック163の暗号化処理サブブロック187は、フラッシュメモリ185に記憶されている使用権情報からメタ鍵を取得し、メタ鍵を利用して、データ送受信ブロック161がコンテンツデータ3とともに受信した暗号化鍵（コンテンツデータ3用）を復号する。

【0201】暗号化処理サブブロック187は、復号して取得した暗号化鍵（コンテンツデータ3用）を利用して暗号化されているコンテンツデータ3を復号する。

【0202】次に、サービスサーバ54から送信されるコンテンツデータに、図19（B）のメタデータ4が対応されている場合のマイクロプロセッサ182の処理について説明する。

【0203】マイクロプロセッサ182は、メタデータ4に記述されている内容から、DESの暗号化アルゴリズムにより暗号化されたコンテンツデータ4を復号する処理能力が要求され、MPEG2の規格で圧縮されたビデオデータをストリーミングの利用形態により再生する場合、4Mbpsの転送速度が要求されていると認識する。

【0204】マイクロプロセッサ182は、自分自身の処理能力と、要求される処理能力を比較した結果、暗号化処理ブロック163が、単独でコンテンツデータ4を処理することは不可能と認識する。この場合、ステップS108において、マイクロプロセッサ182は分散処理が必要であると判定し、処理はステップS111に進む。

【0205】ステップS111において、マイクロプロセッサ182は、コンテンツデータ4の分散処理が必要であるとコントローラ162に通知する。この通知には、コンテンツデータ4の分散処理を行うために必要な情報が含まれる。例えば、コンテンツデータを復号する際に必要なアルゴリズム、暗号化処理ブロック163に不足しているデータの処理速度、および分散処理先による復号関連処理の処理結果の出力先などの情報が含まれる。

【0206】ステップS112において、コントローラ162は、マイクロプロセッサ182から通知された情報に基づいて、コンテンツデータ4の分散処理先を検索する。分散処理先の候補は、コントローラ162にリスト化されて予め与えられおり、この例の場合、ステップ

S113において、コントローラ162自身が、コンテンツデータ4の分散処理先として検索される。

【0207】ここで、マイクロプロセッサ182が要求する処理能力は、コンテンツデータ4のDESによる復号処理結果を2Mbpsで出力、および復号したデータを外部RAM165の所定のメモリ領域への転送とする。

【0208】ステップS114において、コントローラ162は、ソフトウェアにより復号処理を行うため、コンテンツデータ4の復号処理の準備としてソフトウェアプロセスを生成する。

【0209】ステップS115において、コントローラ162のソフトウェアプロセスは、マイクロプロセッサ182に、コンテンツデータ4の分散処理が可能であると通知する。

【0210】ステップS116において、マイクロプロセッサ182は、ソフトウェアプロセスと相互認証を行い、ステップS117で、相互認証が成立したか否かがマイクロプロセッサ182により判定される。

【0211】ステップS117において、マイクロプロセッサ182が、ソフトウェアプロセスと相互認証が成立していないと判定した場合、マイクロプロセッサ182は、コンテンツデータ4を復号することができないと認識し、コントローラ162に相互認証が成立していないと通知する。通知を受け取ったコントローラ162は、利用者55に対して、コンテンツデータ4を復号することができないことを通知し、処理を終了する。

【0212】ステップS117において、マイクロプロセッサ182は、ソフトウェアプロセスと相互認証が成立したと判定した場合、処理はステップS118に進み、マイクロプロセッサ182は、コンテンツデータ4の分散処理の準備が完了したとコントローラ162に通知する。

【0213】ステップS119において、マイクロプロセッサ182からコンテンツデータ4の分散処理の準備が完了したことの通知を受け取ったコントローラ162は、サービスサーバ54に対してコンテンツデータ4の送信を要求する。

【0214】ステップS120において、データ送受信ブロック161は、ネットワーク22を介してサービスサーバ54から送信されてくるコンテンツデータ4を受信する。その後、コントローラ162は、決定した分散処理形式に基づいて、コンテンツデータ4を暗号化処理ブロック163、およびソフトウェアプロセスに対して分配する。

【0215】ステップS121において、暗号化処理ブロック163は、ソフトウェアプロセスに対して、予め指定した分散処理結果の出力先である外部RAM165から、ソフトウェアプロセスの処理結果を取得し、自分自身が復号したコンテンツデータ4とともに、データ再生装置152に転送する。これにより、利用者55はコン

10

20

30

40

50



テンツデータ4を利用することが可能となる。

【0216】以下、コンテンツデータを様々な方式により分散処理する場合のSTB151の処理を説明する。なお、暗号化処理ブロック163の復号関連処理の処理能力は、上述した例の場合と同様に、DESの暗号化アルゴリズムに対応しており、復号したデータの転送速度は3Mbpsとする。なお、以下の説明において、図23乃至図25のフローチャートで、STB151が、メタデータ3およびメタデータ4を有するコンテンツデータを受信した場合と同一の処理については、その説明は、適宜、省略する。

【0217】STB151が受信するデータは、図26に示すフォーマットで構成されており、サービスサーバ54のデータ記憶装置116に記憶されている。図26を図17と比較して明らかなように、この例では、レイヤ2の暗号化単位ブロックはさらに、レイヤ3としての、512KBのデータ長のブロックと、デジタル署名とで構成されている。従って、この例では、この暗号化データに付加されているデジタル署名を検証することにより、コンテンツデータの各暗号化単位ブロックに、改竄などの不正処理が行われているか否かを判断することができる。

【0218】次に、STB151が、図27に示すメタデータ5に対応するコンテンツデータ5を受信した場合の処理について説明する。始めに、メタデータ5について説明する。フィールド1には、サービスプロバイダIDが1、コンテンツIDが1、コンテンツデータ5の著作権発生日時が西暦2000年1月1日として、それぞれ記述されている。

【0219】フィールド2には、コンテンツデータ5の利用形態1としてストリーミング、利用形態2として買い取り、利用形態3として期間限定1年が、それぞれ記述されている。

【0220】フィールド3には、コンテンツデータ5の料金が、ストリーミングの利用形態によりコンテンツデータ5を利用した場合は30円と、買い取りの利用形態による利用の場合は150円と、期間限定1年の利用形態による利用の場合は80円と記述されている。

【0221】フィールド4には、コンテンツデータ5のデータ再生装置152における再生時間は10分であり、総データ量は225MBであると記述されている。また、コンテンツデータ5は、MPEG-2の規格で圧縮されているビデオデータであり、3Mbpsの転送速度が要求されている。

【0222】フィールド5には、デジタル署名の生成アルゴリズムはDSA、コンテンツデータ5の暗号化アルゴリズムはDES、および暗号化のデータ単位は512KBであり、暗号化ブロック毎にデジタル署名が付加されていることが記述されている。

【0223】マイクロプロセッサ182がメタデータ5

を受信した場合、マイクロプロセッサ182は、メタデータ5に記述されている内容から、データ再生装置152において、コンテンツデータ5を再生するために必要なデータ転送速度は3Mbpsであると認識する。そのため、マイクロプロセッサ182は、暗号化処理ブロック163に要求される処理が復号処理のみである場合、暗号化処理ブロック163が、単独で復号処理することが可能であると認識する。ところが、マイクロプロセッサ182は、コンテンツデータ5の暗号化ブロックには、デジタル署名が付加されているため、デジタル署名の検証処理も要求されていると認識し、単独でコンテンツデータ5を処理することは不可能であると判断する。

【0224】上述したメタデータ3および4の場合と同様に、コントローラ162自身により、コントローラ162のソフトウェアプロセスが分散処理先として検索され、マイクロプロセッサ182は、ソフトウェアプロセスに対して、コンテンツデータ5の分散処理を要求する。この場合の要求内容は、512KBの暗号化データ毎に付加されているデジタル署名を検証し、不正処理が存在しているか否かを暗号化処理ブロック163に通知するものである。

【0225】その後、コンテンツデータ5が受信された場合、コンテンツデータ5の復号関連処理は、コントローラ162により分配され、暗号化処理ブロック163はコンテンツデータ5を復号する。一方、ソフトウェアプロセスはデジタル署名の検証を行う。以上の方法で、コンテンツデータ5の分散処理が達成される。

【0226】ソフトウェアプロセスが、デジタル署名の検証処理において、データの不正処理を検出した場合、暗号化処理ブロック163に対して不正処理を検出した旨の通知をするとともに、処理を中止する。

【0227】暗号化処理ブロック163は、コントローラ162から不正処理を検出した旨の通知を受け取った場合、処理の経緯をフラッシュメモリ185に記憶して処理を終了する。記憶された処理の経緯は、後日、決済センタ57に通知され、使用権情報を購入する際に決済された代金が取り消される。

【0228】次に、STB151が、図28に示すメタデータ6に対応するコンテンツデータ6を受信した場合の処理について説明する。始めに、メタデータ6について説明する。フィールド1乃至フィールド4の記述は、図27のメタデータ5と同一であり、その説明は、適宜、省略する。

【0229】フィールド5には、デジタル署名の生成アルゴリズムはDSA、コンテンツデータ6の暗号化アルゴリズムはIDEA(International Data Encryption Algorithm)、暗号化のデータ単位は512KBであり、暗号化ブロック毎にデジタル署名が付加されていると記述されている。

【0230】マイクロプロセッサ182がメタデータ6

を受信した場合、マイクロプロセッサ182は、メタデータ6に記述されている内容から、コンテンツデータ6を復号するためにはIDEAの暗号化アルゴリズムに対応している必要があると認識する。そのため、マイクロプロセッサ182は、DESの暗号化アルゴリズムにのみ対応している暗号化処理ブロック163が、単独でコンテンツデータ6を復号することは不可能であると認識し、コントローラ162のソフトウェアプロセスに復号処理を委託する。

【0231】その後、ソフトウェアプロセスによるコンテンツデータ6の復号処理が行われ、コントローラ162は、処理結果をデータ再生装置152に転送する。

【0232】次に、STB151が、図29に示すメタデータ7に対応するコンテンツデータ7を受信した場合のマイクロプロセッサ182の処理について説明する。この例においては、暗号化処理ブロック163は、コンテンツデータ7の復号処理以外に、他のリアルタイム処理が要求された場合に、分散処理を行うように設定されているとする。また、暗号化処理ブロック163は、外部RAM165に自由にアクセスすることが可能であるとす

る。

【0233】さらに、マイクロプロセッサ182は、内部クロックを有しているとする。内部クロックにより、マイクロプロセッサ182は、所定の時間間隔で、分散処理を指令したコントローラ162のソフトウェアプロセスによる復号処理が、要求内容に基づいて行われているか否かを判断することができる。始めに、メタデータ7について説明する。フィールド1乃至フィールド3、およびフィールド5の記述は、図27のメタデータ5と同一であり、その説明は、適宜、省略する。

【0234】フィールド4には、コンテンツデータ7の再生時間は10分であり、総データ量は300MBであると記述されている。また、コンテンツデータ7はMPEG2の規格で圧縮されているビデオデータであり、2.5Mbpsの転送速度が要求されている。

【0235】マイクロプロセッサ182は、メタデータ7を受信した場合、メタデータ7に記述されている内容から、データ再生装置152においてコンテンツデータ7を再生するために必要なデータ転送速度は2.5Mbpsであると認識する。そのため、暗号化処理ブロック163が単独でコンテンツデータ7を復号することは可能であるが、この例における暗号化処理ブロック163には、コンテンツデータ7の復号処理以外に、他のリアルタイム処理が要求された場合に、分散処理を行うように設定されている。そのため、暗号化処理ブロック163は、暗号化データ毎に付加されているデジタル署名の検証処理が要求されていると認識し、コントローラ162のソフトウェアプロセスに対して、コンテンツデータ7の分散処理を要求する。

【0236】マイクロプロセッサ182は、分散処理の

要求とともに、コンテンツデータ7の処理結果を外部RAM165の所定のアドレス空間に転送することを指定する。その後、コンテンツデータ7がデータ送受信ブロック161により受信された場合、コントローラ162のソフトウェアプロセスは、コンテンツデータ7の暗号化データ毎に付加されているデジタル署名を検証する。

【0237】マイクロプロセッサ182は、自分自身の内部に配置されている内部クロックにより、暗号化処理ブロック163の内部処理が、所定時間毎に終了するようにタイムスケジュールを設定することが可能である。マイクロプロセッサ182は、その設定により、暗号化処理ブロック163の内部処理の空き時間に、外部RAM165にアクセスする。ソフトウェアプロセスは、マイクロプロセッサ182から外部RAM165の所定のアドレス空間に処理結果を転送することを指示されているため、マイクロプロセッサ182は、外部RAM165の所定のアドレス空間にアクセスすることにより、分散処理によるデジタル署名の検証がソフトウェアプロセスにより、要求に基づいて行われているか否かを判断することが可能となる。

【0238】マイクロプロセッサ182は、外部RAM165の所定のアドレス空間から、ソフトウェアプロセスによるコンテンツデータ7の処理結果が取得できないと認識した場合、または分散処理が要求通りに実行されていないと認識した場合、コントローラ162に、分散処理が要求通りに実行されていないことを通知する。その後、コントローラ162は処理を終了する。

【0239】なお、本発明はデジタルデータを処理する様々な装置に適用可能である。以上の例においては、コンテンツデータの分散処理は、STB151の内部に配置されている情報処理部に委託して処理することとしたが、IEEE (The Institute of Electrical and Electronics Engineer, Inc) 1394などの通信インタフェースを介してデータを送受信することが可能である場合、外部の装置に配置されている情報処理部に分散処理を委託することもできる。

【0240】上述した一連の処理は、ハードウェアにより実行させることもできるが、ソフトウェアにより実行させることもできる。一連の処理をソフトウェアにより実行させる場合には、そのソフトウェアを構成するプログラムが、専用のハードウェアに組み込まれているコンピュータ、または、各種のプログラムをインストールすることで、各種の機能を実行することが可能な、例えば汎用のパーソナルコンピュータや、STB151などに、記録媒体からインストールされる。

【0241】図30は、一連の処理を実行するソフトウェアがインストールされるパーソナルコンピュータ201の構成例を示している。パーソナルコンピュータ201は、CPU(Central Processing Unit)211を内蔵している。CPU211にはバス214を介して、入出力イン

タフェース215が接続されている。入出力インタフェース215には、キーボード、マウスなどの入力デバイスよりなる入力部216、処理結果としての例えば音声信号を出力する出力部217、処理結果としての画像を表示するディスプレイなどよりなる表示部218、プログラムや各種データを格納するハードディスクドライブなどよりなる記憶部219、LAN(Local Area Network)やインターネットを介してデータを通信するモデムなどよりなる通信部220、および、磁気ディスク222（フロッピーディスクを含む）、光ディスク223（CD-ROM(Compact Disc-Read Only Memory)、DVD(Digital Versatile Disc)を含む）、光磁気ディスク224（MD(Mini Disc)を含む）、もしくは半導体メモリ225などの記録媒体に対してデータを読み書きするドライブ221が接続されている。バス214には、ROM(Read Only Memory)212およびRAM213が接続されている。

【0242】一連の処理を実行するソフトウェアは、磁気ディスク222、光ディスク223、光磁気ディスク224、および半導体メモリ225に格納された状態でパーソナルコンピュータ201に供給され、ドライブ221によって読み出されて、記憶部219に内蔵されるハードディスクドライブにインストールされる。記憶部219にインストールされているエージェントプログラムは、入力部216に入力されるユーザからのコマンドに対応するCPU211の指令によって、記憶部219からRAM213にロードされて実行される。

【0243】なお、本明細書において、記録媒体に記録されるプログラムを記述するステップは、記載された順序に従って時系列的に行われる処理はもちろん、必ずしも時系列的に処理されなくとも、並列的あるいは個別に実行される処理をも含むものである。

【0244】また、本明細書において、システムとは、複数の装置により構成される装置全体を表すものである。

【0245】

【発明の効果】以上のように、本発明の情報処理装置、情報処理方法、および記録媒体のプログラムによれば、コンテンツデータの特徴情報から、コンテンツデータのデータ処理に要求される処理能力を認識し、データ処理に要求される処理能力と、自分自身の処理能力を比較し、自分自身の処理能力が、データ処理に要求される処理能力を充足していない場合、所定のデータ処理部だけでなく、他のデータ処理部とコンテンツデータを分散して処理するようにしたので、低コストで、かつ、機能変更が容易な、迅速にデータを処理することができるシステムを実現することが可能になる。

【図面の簡単な説明】

【図1】従来の復号LSIの構成例を示すブロック図である。

【図2】本発明を適用したデータ処理システムの構成例

を示すブロック図である。

【図3】データ送信装置の処理を説明するフローチャートである。

【図4】データ受信装置の処理を説明するフローチャートである。

【図5】データ受信装置の処理を説明する図3の続きのフローチャートである。

【図6】本発明を適用したコンテンツ配信システムの概念を示す図である。

【図7】コンテンツサーバの構成例を示すブロック図である。

【図8】データ暗号化装置の詳細な構成例を示すブロック図である。

【図9】サービスサーバの構成例を示すブロック図である。

【図10】決済サーバの構成例を示すブロック図である。

【図11】利用者端末の構成例を示すブロック図である。

【図12】セットトップボックスの構成例を示すブロック図である。

【図13】暗号化処理ブロックの詳細な構成例を示すブロック図である。

【図14】暗号化処理ブロックが送受信するデータ形式の例を示す図である。

【図15】コンテンツサーバの処理を説明するフローチャートである。

【図16】コンテンツサーバが生成するメタデータの例を示す図である。

【図17】コンテンツサーバが送信するデータのフォーマットの例を示す図である。

【図18】サービスプロバイダの処理を説明するフローチャートである。

【図19】サービスサーバが生成するメタデータの例を示す図である。

【図20】決済サーバの使用権情報の発行処理を説明するフローチャートである。

【図21】決済サーバの使用権情報の発行処理を説明する図19の続きのフローチャートである。

【図22】使用権情報の例を示す図である。

【図23】セットトップボックスの処理を説明するフローチャートである。

【図24】セットトップボックスの処理を説明する図22の続きのフローチャートである。

【図25】セットトップボックスの処理を説明する図23の続きのフローチャートである。

【図26】データのフォーマットの例を説明する図である。

【図27】メタデータの例を示す図である。

【図28】メタデータの他の例を示す図である。

【図29】メタデータのさらに他の例を示す図である。

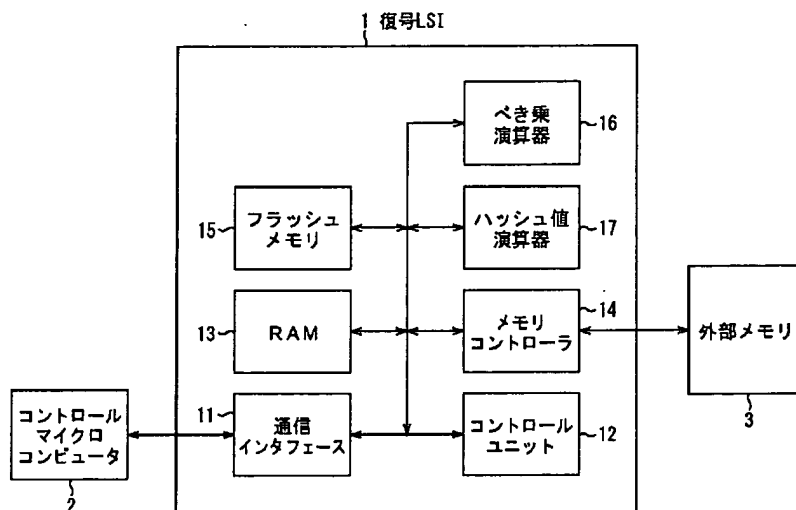
【図30】パーソナルコンピュータの構成例を示すブロック図である。

【符号の説明】

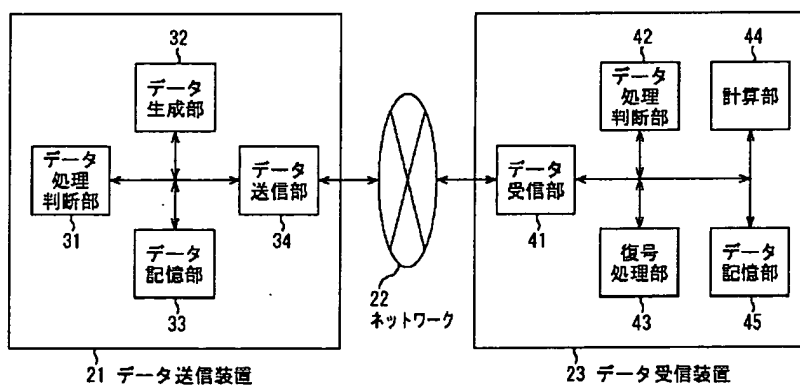
21 データ送信装置、 22 ネットワーク、 23 データ受信装置、 41 データ受信部、 42 データ処理判断部、 43 復号処理部、 44 計算部、 45 データ記憶部、 56 利用者端末、 151 セットトップボックス、 152 データ再生装置、 \*

161 データ送受信ブロック、 162 コントローラ、 163 暗号化処理ブロック、 164 フラッシュメモリ、 165 外部RAM、 181 入出力インタフェースブロック、 182 マイクロプロセッサ、 183 RAM、 184 乱数生成ブロック、 185 フラッシュメモリ、 186 暗号化処理部、 187 暗号化処理サブブロック、 188 デジタル署名検証サブブロック、 189 ハッシュ値計算サブブロック

【図1】



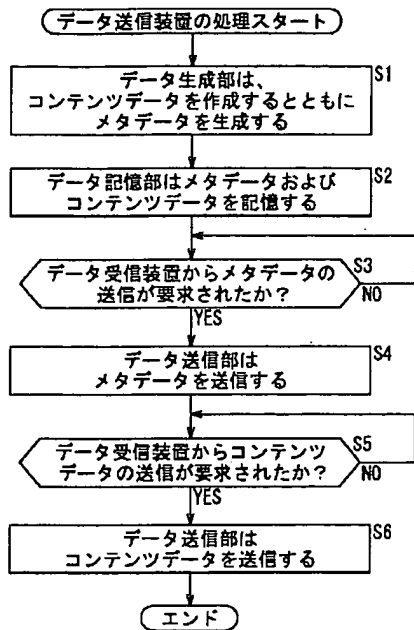
【図2】



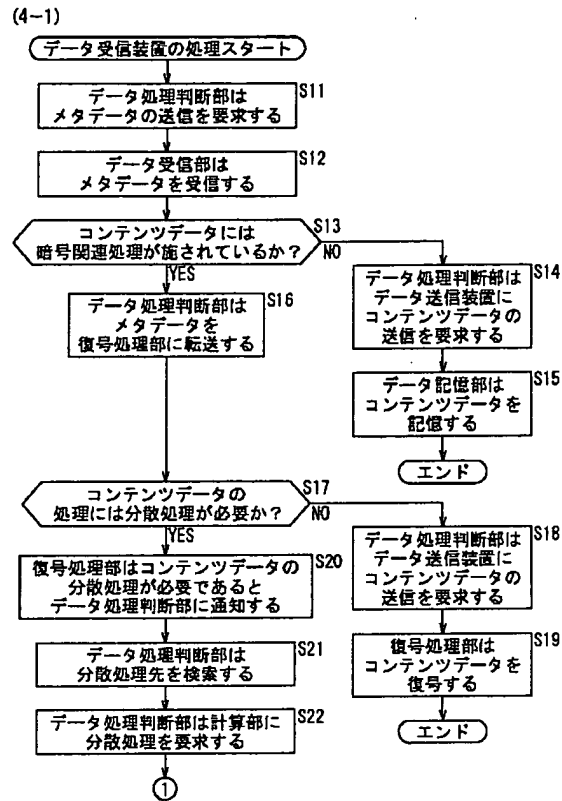
【図14】

フィールド1	フィールド2	フィールド3	フィールド4
データ種識別フィールド	データ番号フィールド	データ長フィールド	データフィールド

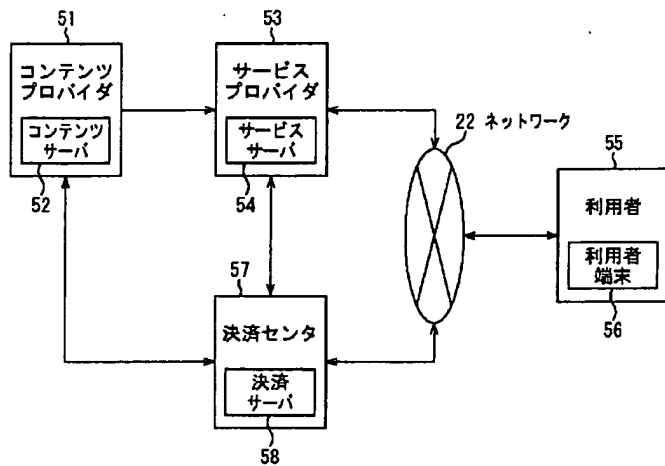
【図3】



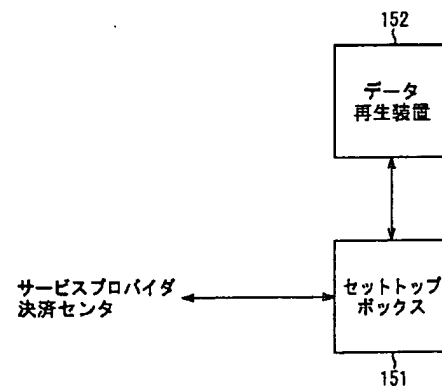
【図4】



【図6】



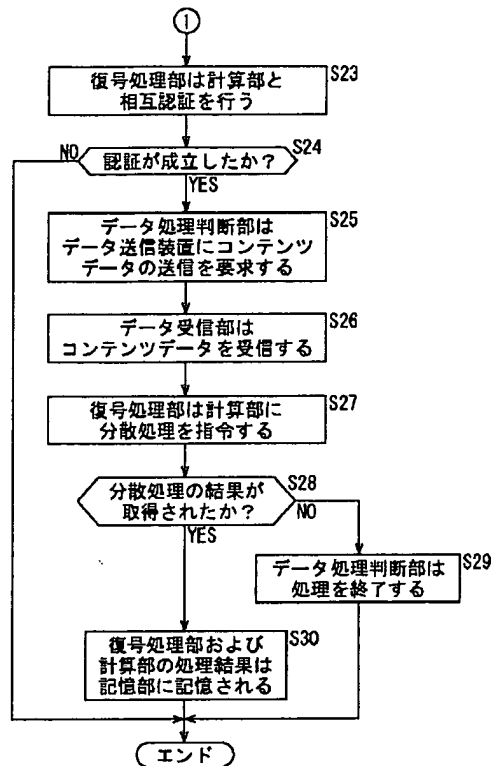
【図11】



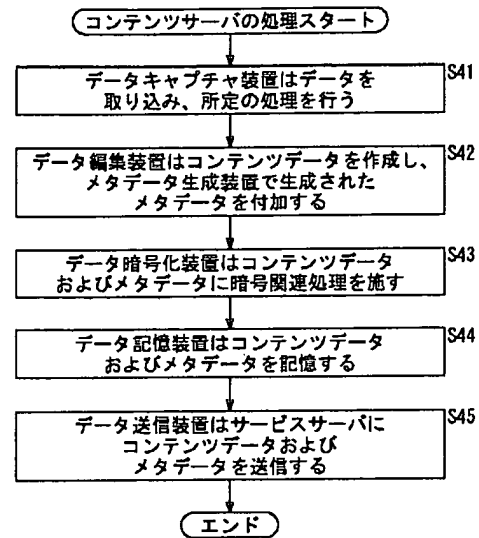
利用者端末 56

【図5】

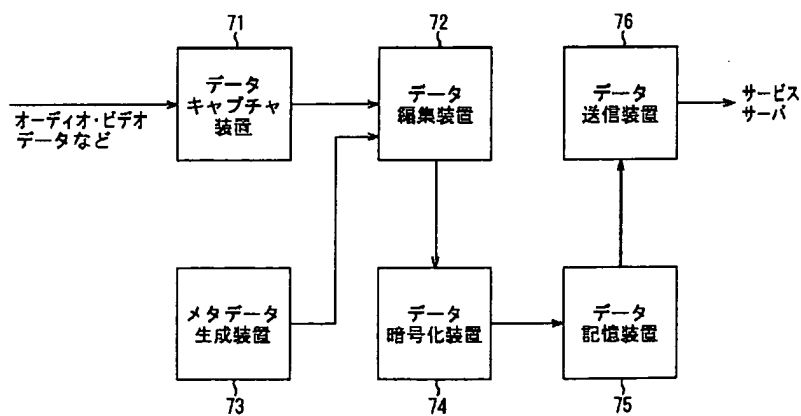
(4-2)



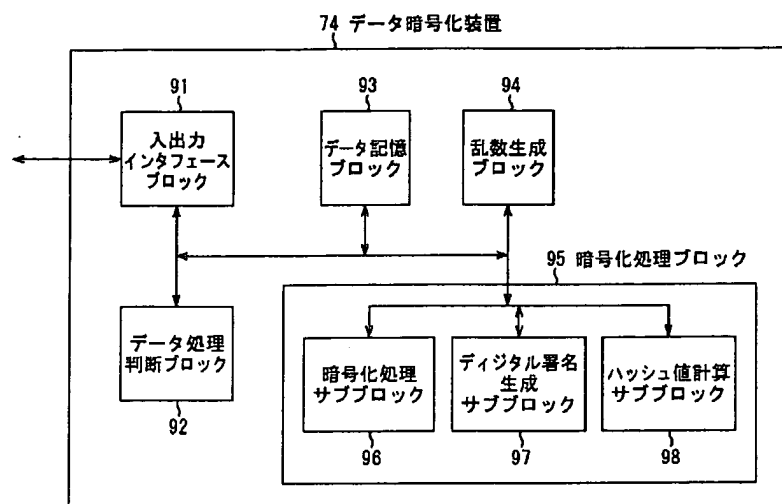
【図15】



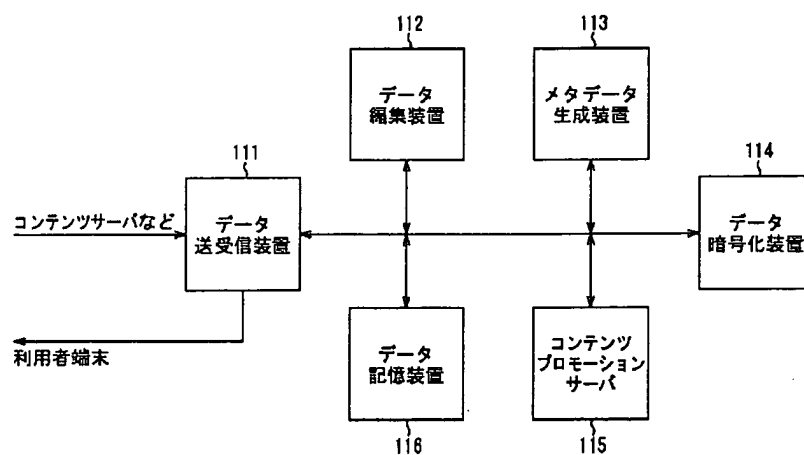
【図7】



【図8】

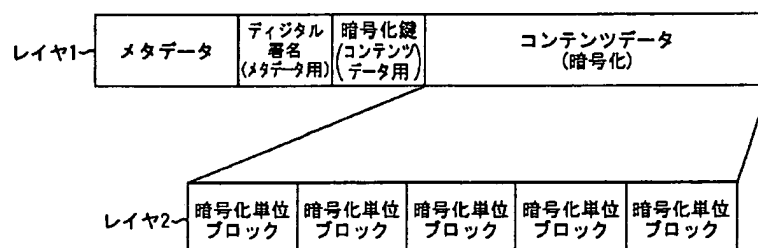


【図9】

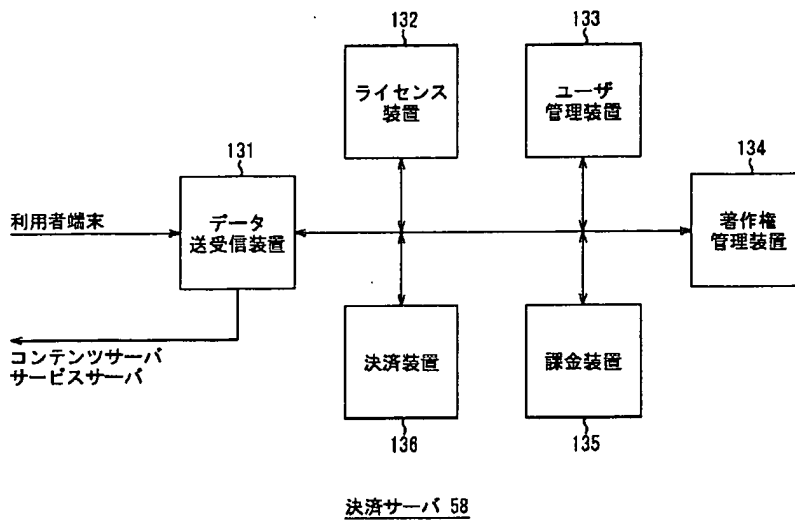


サービスサーバ 54

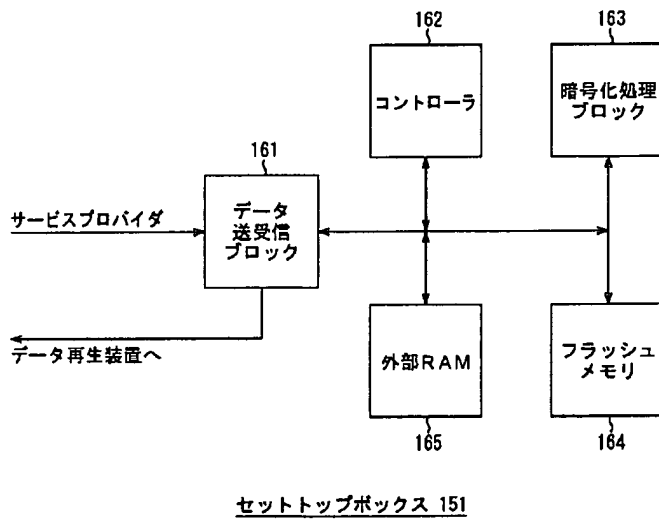
【図17】



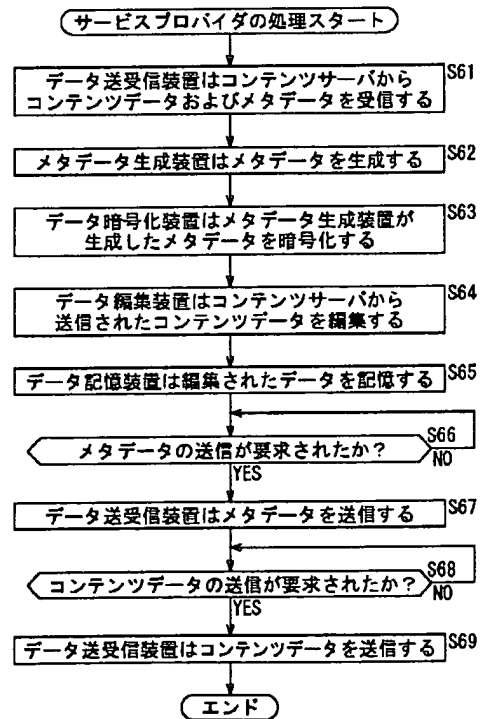
【図10】



【図12】

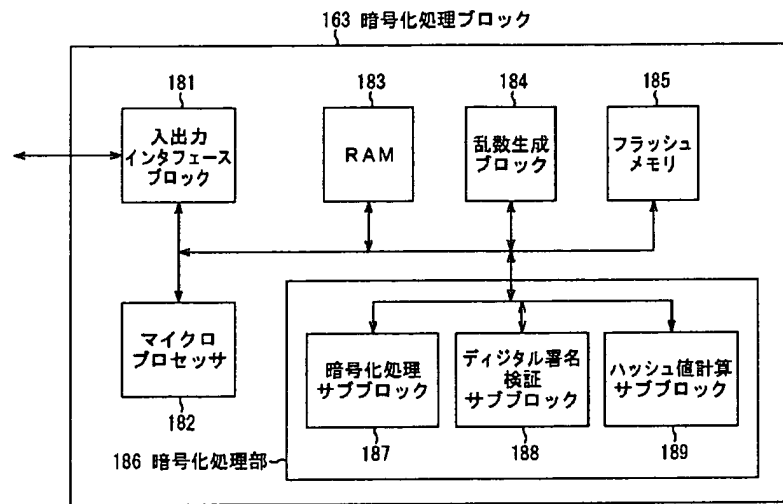


【図18】





【図13】



【図16】

フィールド1	フィールド2	フィールド3	フィールド4	フィールド5
コンテンツプロバイダID 2 コンテンツID 1 権利発生日時 2000年 1月1日	1 ストリーミング 2 買い取り	1 ¥20 2 ¥100	再生時間 10分 総データ量 57.6MB データ形式 MP3 オーディオデータ 転送速度 128Kbps	デジタル署名 DSA 暗号化 DES データ単位 64KB

(A) メタデータ1

フィールド1	フィールド2	フィールド3	フィールド4	フィールド5
コンテンツプロバイダID 2 コンテンツID 2 権利発生日時 2000年 1月1日	1 ストリーミング 2 買い取り 3 期間限定1年	1 ¥20 2 ¥100 3 ¥50	再生時間 10分 総データ量 300MB データ形式 MPEG2 ビデオデータ 転送速度 4Mbps	デジタル署名 DSA 暗号化 DES データ単位 256KB

(B) メタデータ2

【図22】

フィールド1	フィールド2	フィールド3	フィールド4	フィールド5
コンテンツプロバイダID 2 コンテンツID 1 権利発生日時 2000年 1月1日	1 ストリーミング	1 ¥30	メタ鍵	デジタル署名

【図19】

フィールド1	フィールド2	フィールド3	フィールド4	フィールド5
サービスプロバイダID 2 コンテンツID メタデータ作成日時 2000年 1月2日	1 ストリーミング 2 買い取り	1 ¥30 2 ¥150	再生時間 10分 総データ量 57.6MB データ形式 MP3 オーディオデータ 転送速度 128Kbps	デジタル署名 DSA 暗号化 DES データ単位 64KB

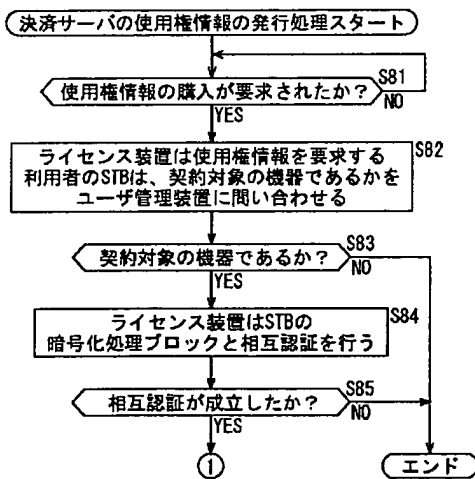
(A) メタデータ3

フィールド1	フィールド2	フィールド3	フィールド4	フィールド5
サービスプロバイダID 2 コンテンツID 1 メタデータ作成日時 2000年 1月2日	1 ストリーミング 2 買い取り 3 期間限定1年	1 ¥30 2 ¥150 3 ¥80	再生時間 10分 総データ量 300MB データ形式 MPEG2 ビデオデータ 転送速度 4Mbps	デジタル署名 DSA 暗号化 DES データ単位 256KB

(B) メタデータ4

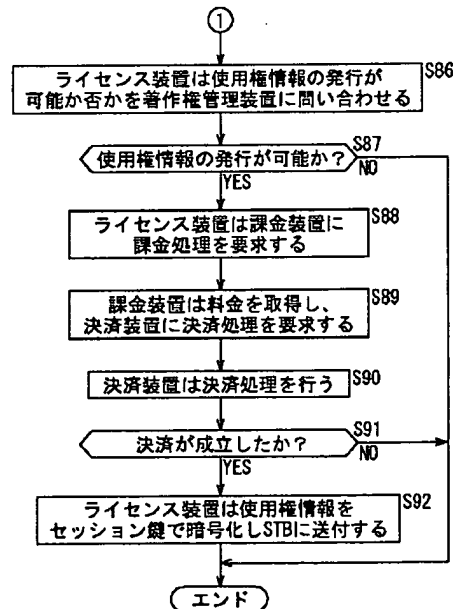
【図20】

(20-1)



【図21】

(20-2)



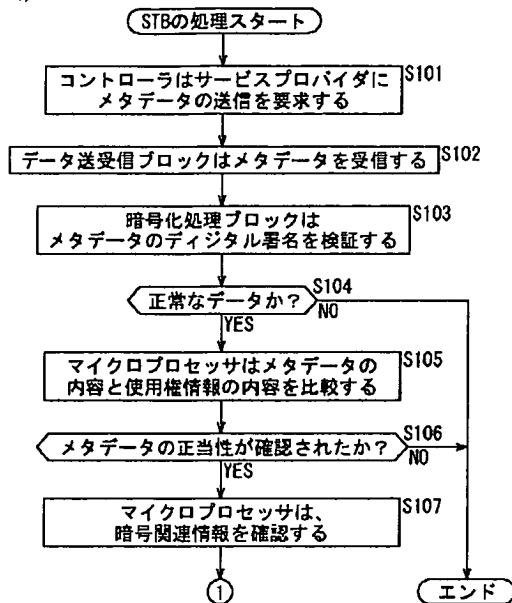
【図27】

フィールド1	フィールド2	フィールド3	フィールド4	フィールド5
サービスプロバイダID 1 コンテンツID 1 メタデータ作成日時 2000年 1月2日	1 ストリーミング 2 買い取り 3 期間限定1年	1 ¥30 2 ¥150 3 ¥80	再生時間 10分 総データ量 225MB データ形式 MPEG2 ビデオデータ 転送速度 3Mbps	デジタル署名 DSA 暗号化 DES データ単位 512KB (署名付)

メタデータ5

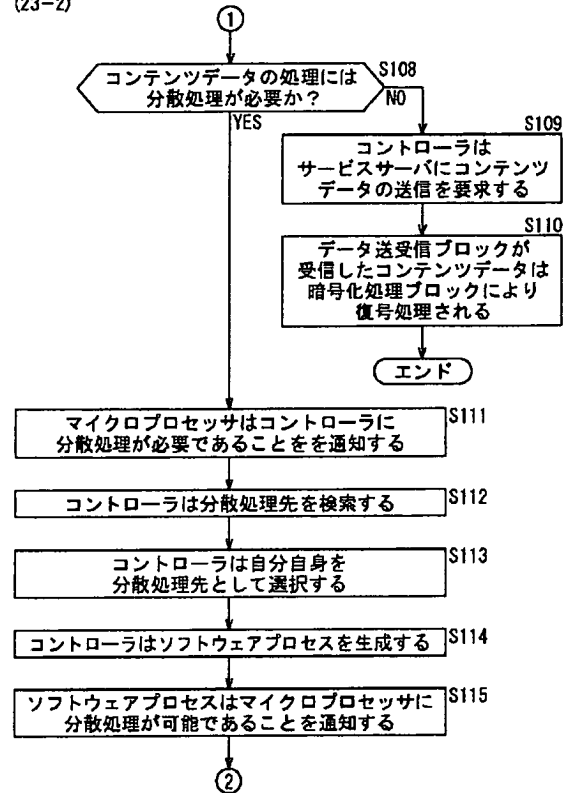
【図23】

(23-1)



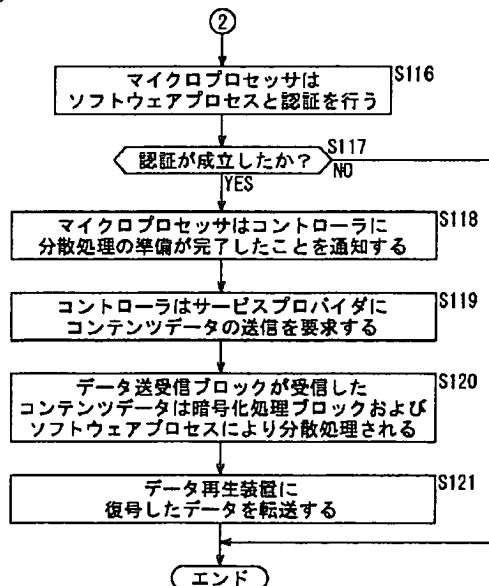
【図24】

(23-2)

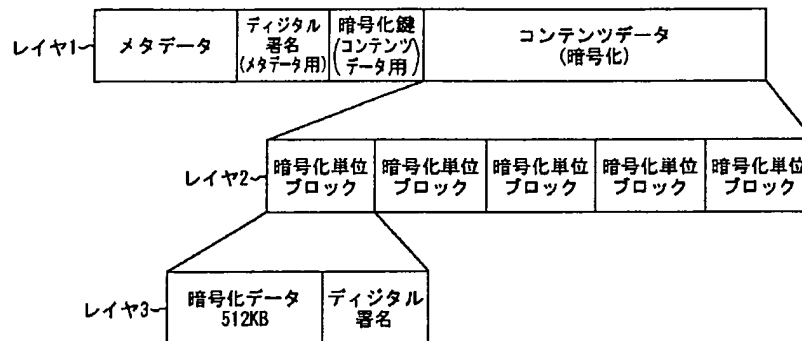


【図25】

(23-3)



【図26】



【図28】

フィールド1	フィールド2	フィールド3	フィールド4	フィールド5
サービスプロバイダID 1 コンテンツID 1 メタデータ作成日時 2000年1月2日	1 ストリーミング 2 買い取り 3 期間限定1年	1 ¥30 2 ¥150 3 ¥80	再生時間 10分 総データ量 300MB データ形式 MPEG2 転送速度 ビデオデータ 2.5Mbps	デジタル署名 DSA 暗号化 IDEA データ単位 512KB (署名付)

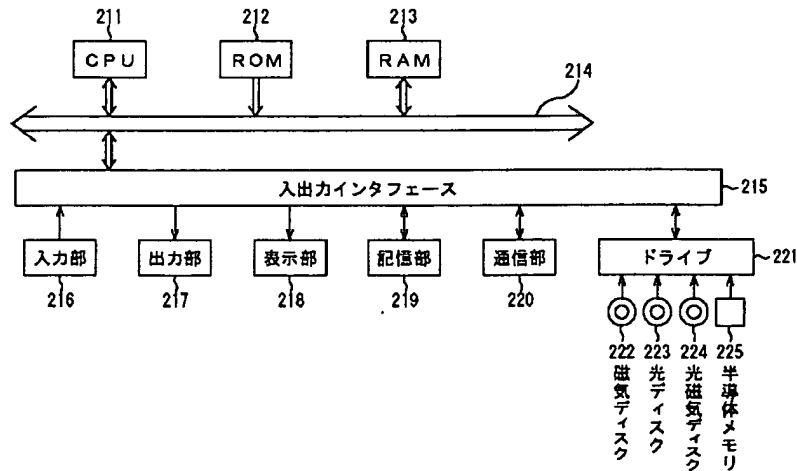
メタデータ6

【図29】

フィールド1	フィールド2	フィールド3	フィールド4	フィールド5
サービスプロバイダID 1 コンテンツID 1 メタデータ作成日時 2000年1月2日	1 ストリーミング 2 買い取り 3 期間限定1年	1 ¥30 2 ¥150 3 ¥80	再生時間 10分 総データ量 300MB データ形式 MPEG2 転送速度 ビデオデータ 2.5Mbps	デジタル署名 DSA 暗号化 DES データ単位 512KB (署名付)

メタデータ7

【図30】



パーソナルコンピュータ 201